HIPAA Faux Pas

Lauren Gluck
Physician's Computer Company
User's Conference 2016

Goals of this course

- Overview of HIPAA and Protected Health Information
- Define HIPAA’s Minimum Necessary Rule
- Properly de-identifying patient information
- Explore 12 HIPAA faux pas and ways to mitigate risk

What is HIPAA?

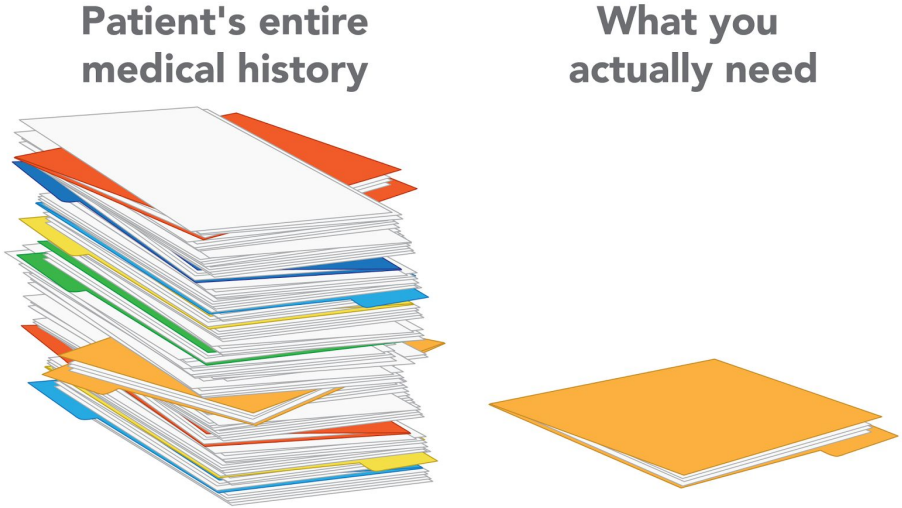
- Health Insurance Portability and Accountability Act originally passed in 1996.
  - Enacted to protect the confidentiality and security of healthcare information
- HIPAA Privacy Rule
  - Establishes standards to protect individuals' medical records and other personal health information
  - Sets limits and conditions on the uses and disclosures of information without patient authorization.
  - Gives patients rights over their health information.
- HIPAA Security Rule
  - Requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and security of electronic protected health information.

What is Protected Health Information?

- Individually Identifiable Health Information
  - Demographic information (name, address, social security number, phone numbers, account numbers, etc)
- Health Information
  - Past, present or future physical or mental health or condition
  - Provision of health care
  - Past, present or future payment for the provision of health care
  - Includes patient's medical record and payment history

Minimum Necessary Rule

- Protected health information (PHI) should not be used or disclosed when it is not necessary to carry out a function.
- Requires evaluation to practices and enhancements to safeguards as needed to limit unnecessary or inappropriate access and disclosure of PHI.



Correctly De-Identifying Health Information

- Correct de-identification requires removing all 18 types of identifiers
- http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#standard

1. Names	
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and equivalent geocodes, excluding initial three digits of a ZIP code if, according to current publicly available data from the Bureau of the Census: a. 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[2]	
3. All elements of dates (except year) for dates directly related to an individual (i.e., birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year)) indicative of such age, except such ages and elements may be aggregated into a single category of age 90 or older.	
4. Telephone numbers 5. E-mail addresses	12. Vehicle identifiers and serial numbers, including license plate numbers
6. Fax numbers	13. Device identifiers and serial numbers
7. Social Security numbers	14. Web Universal Resource Locators (URLs)
8. Medical record numbers	15. Internet Protocol (IP) addresses
9. Health plan beneficiary numbers	16. Biometric identifiers (i.e, finger and voice prints)
10. Account numbers	17. Full-face photographs and any comparable images
11. Certificate/license numbers	18. Any other unique identifying number (i.e., bar codes of patient records and prescriptions), characteristic (i.e., "current president of state university"), or code, except codes that enable re-identification provided the entity does not disclose such code for any other purpose and the mechanism for re-identification.

HIPAA Faux Pas #1: Unauthorized Access

- Reasons for unauthorized access:
  - Personal Reasons
  - High Profile Patient

- Ways to mitigate risk:
  - If using PCC EHR: use patient flag/clinical alert for sensitive patients
  - If using PCC EHR: utilize the new Audit Log tool to audit chart access
  - Ensure employees know privacy policy/consequences for unauthorized access

HIPAA Faux Pas #2: Weak Passwords

- Weak password examples:
  - Anything that is personal to you (name, date of birth, etc)
  - Found in a dictionary
  - Short

- Ways to mitigate risk:
  - Strong password examples:
    - At least 8 characters
    - Does not contain your name or a complete word
    - Contains some different characters (uppercase letters, numbers, symbols)
  - PCC EHR now requires at least 8 characters in a password and it cannot contain the user's name or EHR username

HIPAA Faux Pas #3: Unsecured Workstations/Charts

- Risks:
  - Unauthorized access to charts/information
  - Theft

- Ways to mitigate risk:
  - If using PCC EHR: use the auto logoff feature
  - Workstations should lock after a specified amount of time and require a password to log back into the desktop
  - Workstations and charts should not be left where they are in sight of patients or vulnerable to theft
  - Laptops should be kept in a locked room, drawer or cabinet overnight

HIPAA Faux Pas #4: Storing PHI on flash drives

- Risks:
  - Small and easily stolen
  - Able to download viruses that can compromise data
  - Doesn't automatically record any changes to the data

- Ways to mitigate risk:
  - Don't use flash drives for PHI!!
  - CDs are preferable, but do still carry risks

HIPAA Faux Pas #5: Discussing PHI

- Risks:
  - Incidental Disclosure
    - Not intentional
    - Unavoidable
  - Non-Incidental Disclosure
    - Two types:
      - Accidental
      - Deliberate

- Ways to mitigate risk:
  - PHI should not be discussed in front of other patients or anyone who is not employed by your practice

HIPAA Faux Pas #6: Posting PHI to social media

- Risks:
  - Data breaches
  - Posting data that is not completely de-identified
- Ways to mitigate risk:
  - Don’t post information about injuries or treatments of patients on social media

HIPAA Faux Pas #7: Improper Disposal of PHI

- Risks:
  - Theft
  - Breaches of data

- Ways to mitigate risk:
  - Shred any paper PHI
  - Completely delete ePHI from workstations
  - If hardware is being updated, the old hardware must be wiped clean
  - Partner and PCC EHR do not store any data on individual workstations (unless PHI is manually saved in the form of reports). All data lives on the server.

HIPAA Faux Pas #8: Lack of HIPAA Training for staff

- Risks:
  - Staff is unaware of HIPAA policies
  - Possibility of breaches

- Ways to mitigate risk:
  - All staff should be trained on internal privacy and security policies of the practice
  - Staff should know who serves as the HIPAA officer for the practice

HIPAA Faux Pas #9: Calling a patient's full name

- A patient's full name (even first and last) is PHI

- Ways to mitigate risk:
  - When calling a patient's name into the waiting room call only their first or their last name
  - Discuss other ways to call patients to the window without calling their name:
    - A couple of examples I have seen: giving the patient a number, using a pager that buzzes

HIPAA Faux Pas #10: Disclosing PHI during check in

- PHI potentially disclosed during check in process:
  - Patient's full name
  - Address
  - Insurance
  - Billing Information

- Ways to mitigate risk:
  - Use the minimum necessary rule when confirming information verbally
  - Ensure no other patients are near the window when verifying the information
  - Speak softly so that those in the waiting room cannot hear the information
  - Confirm information using non-verbal means

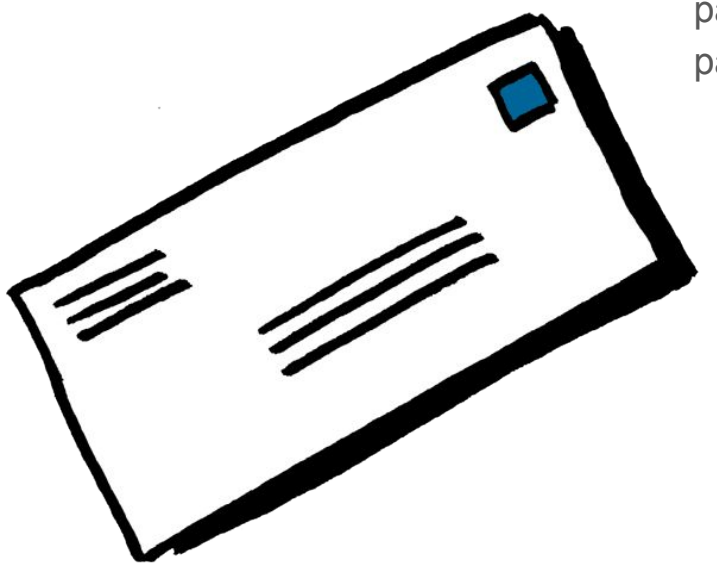
HIPAA Faux Pas #11: Misdirected Emails

- The HIPAA Privacy Rule does not forbid sending PHI over email:
  - http://www.hhs.gov/hipaa/for-professionals/faq/570/does-hipaa-permit-health-care-providers-to-use-email-to-discuss-health-issues-with-patients/
- The HIPAA Privacy Rule does require all necessary precautions to protect the data being sent

- Ways to mitigate risk:
  - Confirm the email address before sending PHI (send test email)
  - Use the minimum necessary rule and send only the data required
  - If someone needs to send you PHI, have them send it to your PCC email address
    - All emails received into your PCC email address live on the server, which is encrypted
  - Google apps are now HIPAA compliant, if you sign a BAA
    - https://**support.google.com**/a/answer/3407054?hl=en

HIPAA Faux Pas #12: Providing incorrect records

- Mailing the incorrect records or paperwork to a patient
- Printing a handout and giving it to the incorrect patient



- Ways to mitigate risk:
  - Review the patient name on all pages before sealing the envelope
  - Review the patient name on all pages before handing the records to patient

HIPAA Risk Assessment and Policies

- Every practice should perform a risk assessment to find potential risks and vulnerabilities that could jeopardize the PHI in their office
- Every practice should have written privacy and security policies and train their staff on both
- Every practice should have a HIPAA officer who is responsible for following up on potential breaches and answering any of the staff's HIPAA questions.
- http://learn.pcc.com/help/hipaa-security-risk-assessments-and-the-pediatric-practice/

Questions?