HIPAA Faux-Pas

Lauren Smith, PMP
2019 User's Conference
Burlington, VT

PCC
Pediatric EHR Solutions

THRIVING
THROUGH
CHANGE

Goals of this course

- Overview of HIPAA and Protected Health Information
- Definition of HIPAA’s Minimum Necessary rule
- Properly De-Identifying patient information
- Explore 10 HIPAA faux-pas and ways to mitigate risk

What is HIPAA?

HIPAA
Health Insurance Portability and Accountability Act

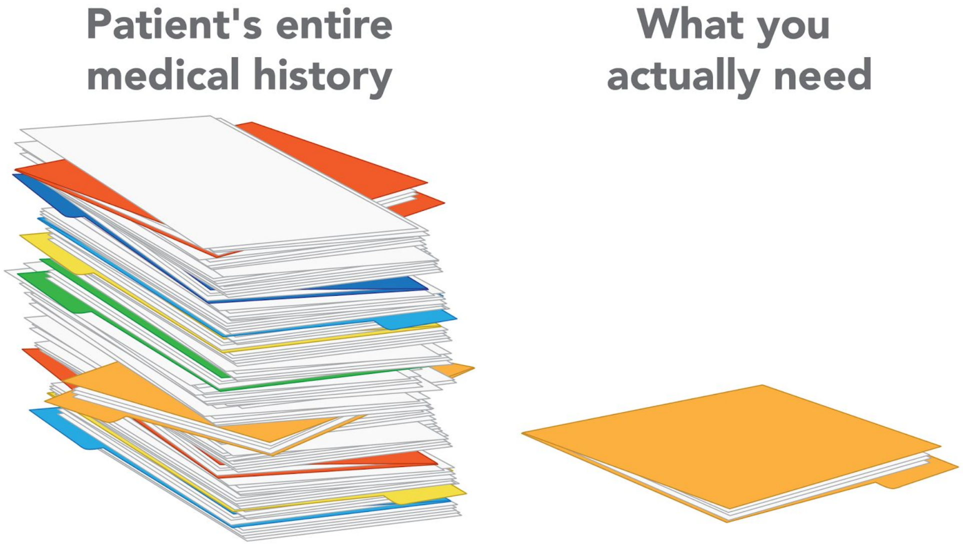
- Health Insurance Portability and Accountability Act originally passed in 1996.
    - Enacted to protect confidentiality and security of healthcare information
- HIPAA Privacy Rule
    - Standards to protect individuals’ medical records and other protected health information (PHI)
    - Sets limits on use and disclosure of PHI without patient permission
    - Patients have rights over their PHI
- HIPAA Security Rule
    - Requires admin, physical and technical safeguards to ensure confidentiality, integrity and security of PHI

What is PHI?

- IIHI (Individually Identifiable Health Information
  - Name, address, SSN, phone numbers, account numbers, etc
- Health Information
  - Diagnoses, charge information, places of treatment, chart notes, etc

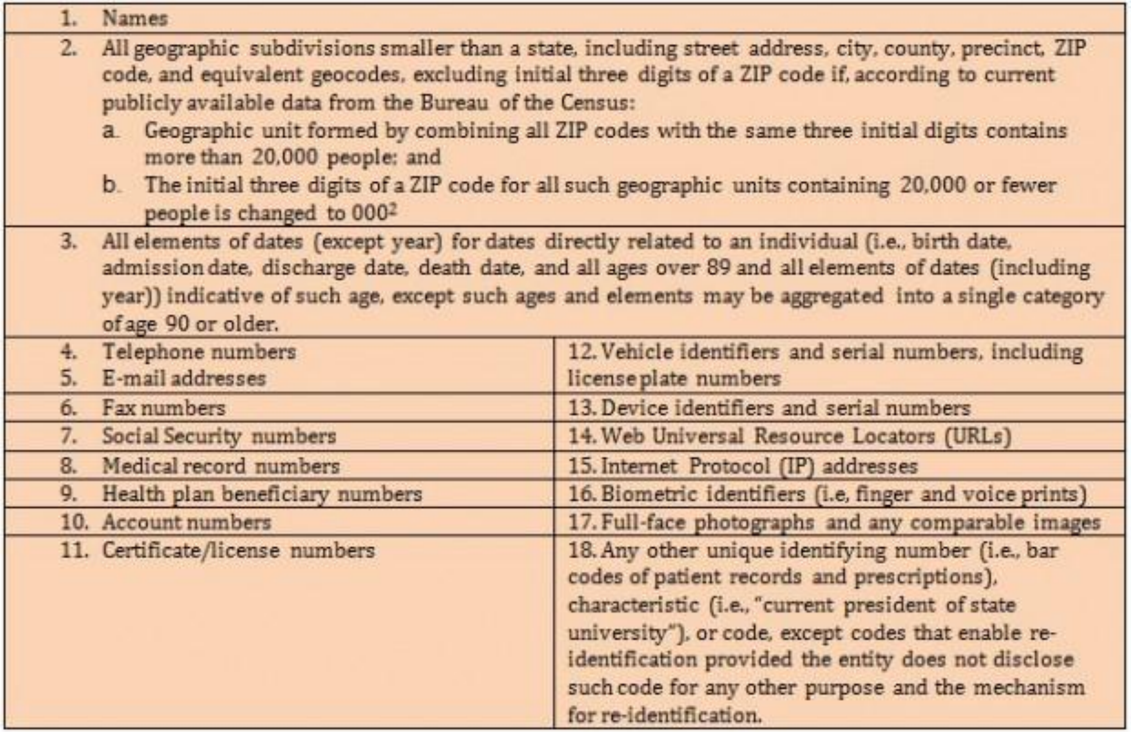
Minimum Necessary Rule

- PHI should not be disclosed when not necessary
- If PHI needs to be shared, ensure it is the minimum amount necessary
  - For example, a patient's health information summary or patient visit summary vs entire visit note



Correctly De-Identifying Health Information

- Correct de-identification requires removing all 18 types of identifiers



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.

PCC Pediatric EHR Solutions

THRIVING THROUGH CHANGE

HIPAA Faux Pas #1: Unauthorized Access

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

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

PCC Pediatric EHR Solutions

THRIVING THROUGH CHANGE

HIPAA Faux Pas #2: Unsecured Workstations/Charts

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

- Ways to mitigate risk:
  - Encrypt laptop hard drives - stolen laptops not considered PHI breach if hard drive is encrypted
  - Use auto logout feature in PCC EHR
  - Workstations should auto lock and require password for re-entry
  - Workstations/charts should not be left unattended around patients
  - Laptops should be kept in a locked room, drawer or cabinet

PCC Pediatric EHR Solutions

THRIVING THROUGH CHANGE

HIPAA Faux Pas #3: Not keeping consent forms up-to-date

- Risks:
  - Releasing information to non-authorized party

- Ways to mitigate risk:
  - Have parents/patients fill out a new form regularly
  - If family situation has changed, ensure a new form is completed
  - Keep track of any expiration dates on authorization the parent/patient has noted on the form

HIPAA Faux Pas #4: Incorrect verbiage when charging for medical record release

- Risks:
  - Patient reports violation to OCR
  - Lost revenue

- Ways to mitigate risk:
  - HIPAA does allow for a fee to cover costs associated with providing patient records. However, that fee ONLY covers the following costs:
    - Labor
    - Supplies (CD, paper, etc)
    - Postage
  - Ensure that when you bill the patient, the fee is an amount for those costs and does not reflect a cost per page/record

PCC Pediatric EHR Solutions

THRIVING THROUGH CHANGE

HIPAA Faux Pas #5: Discussing PHI/Posting to social media

- Risks:
  - Data Breach/Dislosing PHI
    - 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
    - Non-employees
    - Employees not authorized to hear that PHI
  - No posting of PHI to social media
    - Ensure staff is trained on the consequences of disclosing PHI

PCC Pediatric EHR Solutions

THRIVING THROUGH CHANGE

HIPAA Faux Pas #6: Improper Disposal of PHI

- Risks:
  - Theft
  - Data Breach

- Ways to mitigate risk:
  - Shred paper PHI
  - Completely delete PHI from workstations
  - If updating hardware, ensure the hard drive from the old hardware (computers, copiers, etc) is wiped clean

PCC Pediatric EHR Solutions

THRIVING THROUGH CHANGE

HIPAA Faux Pas #7: Providing Incorrect Records

- Risks:
  - Data Breach

- Ways to mitigate risk:
  - Review patient name on all pages before handing to patient/putting in envelope to mail
  - If emailing records ensure that the email address is correct
    - Send a test email first if there is a question about having the correct email address

HIPAA Faux Pas #8: Disclosing PHI during check in

- Risks:
  - Data Breach

- Ways to mitigate risk:
  - Use minimum necessary rule if verbally confirming data
  - Ensure no other patients are near the window
  - Speak softly
  - Confirm information using non-verbal means

PCC Pediatric EHR Solutions

THRIVING THROUGH CHANGE

HIPAA Faux Pas #9: Lack of Privacy/Security policies

- Risks:
  - Violation during HIPAA audit
  - Inability to train staff on HIPAA policies
  - Possibility of breaches

- Ways to mitigate risk:
  - Perform security risk assessment to determine your practice's biggest risks
  - Create internal privacy/security policies
  - Train staff on those policies
  - Update policies as needed
- Documentation available to help with creating these policies:
  - http://learn.pcc.com/help/hipaa-security-risk-assessments-and-the-pediatric-practice/

HIPAA Faux Pas #10: Lack of HIPAA training for staff

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

- Ways to mitigate risk:
  - All staff should be trained on internal privacy/security policies
  - Staff should know who HIPAA officer(s) are
  - Involve everyone in HIPAA - it is not just the responsibility of the HIPAA person, everyone has to help for a practice to be HIPAA compliant

Wrap Up

Take a moment to think if your practice is currently committing any of these faux pas and how you can make changes to mitigate your risks.

Takeaways

What have you learned today that you plan to take back to your office?

Questions?