

HIPAA Presentation for AHEC Residents

August 24, 2009

Vera M. Chenault, J.D.

UAMS HIPAA Campus Coordinator

TPO

HIPAA is not intended to interfere with treatment of patients or to restrict access to patient records for the purpose of making healthcare decisions

Sharing information for the purpose of *treatment, payment, or healthcare operations* (TPO) is always allowed without an authorization

TPO

- As care providers, most of your uses and disclosures will be for treatment purposes.
- Today we will discuss how to navigate issues that might come up within “treatment” as well as some disclosures that you may make for other purposes
- We will discuss also disclosures that are not allowed, and how to prevent them from occurring

Treatment

- Using and disclosing information for treatment purposes means you can share information with other care providers about a mutual patient, you can access the medical records of a patient you are treating in the performance of your job duties, and you can discuss a patient's care with your colleagues to make treatment decisions

Family and Friends

- In the context of treating a patient, you may also share information with your patient's friends and family who are involved in that patient's care
- You should always verify the identity and authority of anyone not known to you prior to disclosing health information about a patient to them

Friends and Family

- If the patient is present or otherwise available prior to the disclosure, you must:
 - Obtain the patient's agreement or
 - Provide the patient an opportunity to object, and they do not or
 - Using professional judgment, reasonably infer from the circumstances that patient does not object.

Friends and Family

- If the patient is not present, or is incapacitated, or in an emergency situation, you may provide:
 - the information directly relevant to family/friend's involvement in the patient's care, *if you determine it is in the patient's best interest.*

Safeguards

- “Incidental disclosures” happen when reasonable safeguards have been taken to protect a patient’s information and a visitor or another patient happens to hear or see the PHI that you are using. You will not be liable for incidental disclosures, provided you are taking reasonable precautions.
- Examples of Safeguards:
 - Do not leave PHI on unattended desks, computer terminals, fax machines, or copiers.
 - If you happen to notice PHI that is left out, don’t read through it; close it, cover it, or put it away.
 - After business hours or when not in use, PHI should be supervised or kept in a locked location.
 - Avoid discussing PHI in public areas such as cafeterias and elevators.
 - If you are discussing a patient on a cell phone, be aware of who is around you and how loudly you are speaking

Safeguards

- More ways to safeguard protected health information
 - Dispose of PHI properly by shredding or placing in a locked shredding bin.
 - Remove patient labels from lab coats or scrub pockets before going outside.
 - When accessing PHI on a computer, be aware of anyone nearby and don't allow them to view your computer screen.
 - Log off or lock your computer prior to stepping away from it

Safeguards

- Electronic PHI
 - Use the password protection and encryption features of your blackberry, cell phone and other mobile devices such as thumb drives and CDs.
 - Guardian Edge (encryption software) is required on laptops and computers containing confidential information – contact IT
 - Encrypt any email containing PHI sent outside UAMS intranet.
 - Always maintain and use passwords in a secure and confidential manner
 - Never share your password or use someone else's sign on information

Patient Authorizations

- Generally, any disclosures other than for *treatment, payment or healthcare operations* require that the patient sign an authorization form
- There are certain exceptions, such as when the disclosure is required by law or made to law enforcement or other agencies, and we will briefly discuss those as they may come up in your practice here

Disclosures *Required* by Law

- There are certain disclosures that are required (not just permitted) by law
- These disclosures may be made without a patient authorization
- However, you must account for the disclosure on the “Accounting for Disclosures” form
- Limit disclosure to only the information required by the law
- Make the disclosure only to those authorities authorized to receive the information under the law

Disclosures Required by Law

- Examples of disclosures required by law
 - Deaths from suspicious circumstances
 - If you have knowledge of a death caused by violence or criminal conduct or other suspicious cause (next slide)
 - Disclosure may be made to county coroner and chief law enforcement official in the county where the death occurred
 - Child maltreatment, abuse, or neglect
 - If you have reasonable cause to suspect child (<18) has been abused or neglected
 - May disclose medical records related to the abuse to the DHS and law enforcement officials
 - Abuse or neglect of elderly, endangered, or impaired adult
 - If you have reasonable cause to suspect endangered or impaired adult, or adult living in long-term care facility, has been abused or neglected
 - May disclose PHI to the DHS, Office of Attorney General, County Prosecutor, County Coroner, and Adult Abuse Hotline

Disclosures Required by Law

- Note that the only categories of patients whose abuse may be reported without their consent are children or certain classes of vulnerable adults
- If a competent adult who has been abused does not consent to having their health information shared with law enforcement, you may not disclose it (unless it falls under one of the other circumstances discussed here)
- You may obtain consent from an adult victim either verbally or in writing

Disclosures Allowed by Law

- Other disclosures to government or other agencies are allowed by law, without a patient authorization
- These must be limited to the amount authorized by the law, may be made only the authorized authorities, and must be limited to the minimum necessary required for the purpose

Disclosures Allowed by Law

- Disclosures for identification and location of suspect, fugitive, material witness or missing person
- To prevent or lessen serious and imminent threat to health or safety
- To report a crime on UAMS property

Unauthorized Disclosures and Special Situations

- “Honey, how was your day?”
- Blogs, social media and networking
- The media
- Access of patient records outside the performance of your job is prohibited
 - This includes your own records and the records of:
 - Family
 - Friends and acquaintances
 - Co-workers

New HIPAA Enforcement

- Changes to HIPAA in the Stimulus Plan
 - Strict liability fines up to \$1 million per occurrence
 - Requirement that we notify the patient and CMS of a “breach” – including inappropriate access to a patient’s record
- Recent criminal prosecutions
 - 2 St. Vincent employees and 1 community physician have plead guilty to federal charges because they snooped in a VIP’s record. They were fired from their jobs and are facing high fines and possible prison time.
 - Other similar cases across the country

Your HIPAA Team

This is why you have us – we are here to protect you and provide you with information and guidance.

<http://hipaa.uams.edu>

Vera Chenault, UAMS HIPAA Campus Coordinator (501-603-1379)

Terry Addison, AHEC Privacy Officer (501) 614-2224

Anita Westbrook, Medical Center Privacy Officer (501-526-6502)

Pamela “Mo” Valentine, Research Privacy Officer (501-526-7559)

Steve Cochran, Security Officer (501-603-1336)

Bill Dobbins, HIPAA Auditor and Educator (501-526-7436)

Kyla Alexander, HIPAA Auditor and Educator (501-614-2098)

Ashley Vestal, HR and Training Coordinator (501-603-1379)