Safeguarding Protected Health Information for the Quality Management Department

Presented by the UAMS HIPAA Office
New HIPAA Enforcement Requirements

Changes to HIPAA as a result of the 2009 Stimulus Bill:

• Strict Liability fines up to $50,000 per incident and up to $1.5 million annually.

• Requirement that we notify DHHS of a “breach” including inappropriate access to a patient’s record.
Any use or disclosure of PHI that is not permitted by the Privacy Rule that poses a significant risk of financial reputational or other harm. For example:

- A UAMS employee accesses the record of a patient outside the performance of their job duties
- An unencrypted laptop containing PHI is lost or stolen
- PHI is sent to the wrong fax, mailing address or printer
Exceptions – there are certain types of uses of disclosures that do not meet the definition of a “breach.” These exceptions are:

- Unintentional use by a UAMS workforce member that does not result in the PHI being further used or disclosed. For example, a nurse accidentally clicks on the wrong patient’s name in WebChart, pulls up that patient’s record, realizes that she is in the wrong patient’s chart, and closes the record.

- Unauthorized disclosure to an individual who cannot possibly retain it. For example, when checking a patient in, you accidentally hand the patient a registration packet that belongs to someone else, but you realize your mistake and immediately retrieve the information.
Notification Requirements

• UAMS must notify every person in writing whose unsecured PHI has been breached as soon as feasible but within 60 days.
• UAMS must report breaches to HHS.
  • If less than 500 individuals, log and report annually.
  • If more than 500 individuals must notify HHS at the same time we notify the patient and we must also notify the media.
How Can You Help?

• Notify the UAMS HIPAA Office as soon as you suspect a possible breach.
• The HIPAA Office will then determine if an actual breach has occurred and take care of the notification process.
• Help us keep patient contact information current.
• Follow your department’s documentation requirements.
• Take steps to prevent breaches from happening in your department.
• When in doubt, just contact us.
UAMS Faxing Policy 3.1.19

• **Confidential** data should be faxed only when mail will not suffice.
• Faxes containing **PHI** and other confidential information must have an official UAMS fax cover sheet.
• Reconfirm recipient’s fax number before transmittal.
• Confirm receipt of fax
• Notify your supervisor/HIPAA Office immediately if a fax is sent in error.
Printed PHI

• Don’t leave PHI “lying around” where others can see it.
• Don’t put PHI, including patient stickers and medication labels, in the regular trash. Shred or place in the privacy bins.
• Obliterate patient information on IV bags or cover with the white labels from the Omnicel before placing in the regular trash.
• When retrieving information from the printer and mailing/faxing information, check every page to make sure it is the correct patient.
Communicate Quietly

- Make it a habit – always lower your voice when discussing patient information.
- Be considerate of patient privacy at the nurse’s station.
- Try to discuss patients privately.
- Stop the conversation if someone walks up.
Use and Disclosure 3.1.28

- Generally, you may use and disclose PHI for treatment, payment and healthcare operations (TPO) of our organization WITHOUT patient authorization.

- In your role, most of your uses (within UAMS) and disclosures (outside UAMS) of PHI, will be for UAMS Healthcare Operations purposes. (See attached definition)

- If the requestor is not known to you, always VERIFY their identity and AUTHORITY before providing PHI.
Minimum Necessary 3.1.25

• When using or disclosing PHI or requesting it from another organization, we must make reasonable efforts to limit it to the smallest amount needed to accomplish the task.

• If the entire chart is not required, only ask for and access the information you need.

Follow the simple “need to know” rule.
• HIPAA generally requires that a patient sign an Authorization for disclosures (sharing protected health information – PHI – with someone outside of UAMS) made for purposes other than TPO

• There are certain exceptions to this rule, such as when the disclosure is required or permitted by law, and an authorization is not required in those cases.
Disclosures Required by law

• 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 to Health Oversight Agencies is a “required by law” example.
Health Oversight Agencies

• State or federal agencies authorized by law to oversee the health care system or government programs
• May disclose PHI for health oversight including audits, investigations, inspections, licensure or disciplinary actions
• Examples - Medicare and Medicaid, State licensure boards, and DHHS Office of Inspector General
Accounting of Disclosures 3.1.26

- A patient has the right to receive a record of certain entities we have disclosed their information to.

- Disclosures for UAMS Treatment, Payment, or Health Care Operations are not currently subject to Accounting.

- All of the “required or permitted by law” disclosures are subject to “accounting of disclosures” and you must report the disclosure.
Electronic PHI

Be aware of your computer screen

• Position your monitor or Computer on Wheels (COW) so the screen cannot easily be seen by passersby
• Minimize the screen if someone walks up
• Log off or lock your computer prior to stepping away from it
Electronic PHI

- Use the password protection and encryption features of your blackberry, cell phone and other mobile devices such as thumb drives and CDs.
- Only store PHI on these devices when absolutely necessary for UAMS business purposes and delete it as soon as feasible.
- Easy to use Imation USB 2.0 **Pivot Plus** Flash Drives are available in the Stockroom.
- Guardian Edge (encryption software) is required on laptops and computers containing confidential information.
- Encrypt any email containing PHI sent outside UAMS intranet.
Passwords

• Always maintain and use passwords in a secure and confidential manner
• Never share your password or use someone else’s sign on information
• If you are asked to sign on using someone else’s information, refuse to do so and report them
Patient Photography 3.1.44

• Written consent is required for photos/video taken for the purpose of treatment, payment, and other health care operations such as teaching within UAMS.

• Consent can be combined with other forms such as Consent for Surgery.

• Written authorization is required for photos/video to be disclosed outside UAMS.
Exceptions to Written Consent Requirement Include:

• Photograph taken for identification purposes only
• When a patient requests UAMS staff to make photographs solely for the patient’s personal use
• General recording or filming of premises for security purposes
• If emergency or patient unable to consent, images can only be used for identification or treatment purposes unless consent obtained later.
Security and Storage

• Must be stored in secure manner
• May not be retained on digital cameras, cellular telephones, or other recording devices or storage cards
• Generally considered part of the patient’s health record
Why would the HIPAA Office call me?

• Access to patient records is monitored
• If your name is on an audit report, and the appropriateness is not readily apparent to the auditors, you or your supervisor will be contacted
• This is routine follow-up and is done for physicians, students and staff.
Why would the HIPAA Office call me?

• 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
• Violations of UAMS HIPAA Policies are taken so seriously that your supervisor will be notified and must impose disciplinary action
Recent Criminal Prosecutions

It can happen to you if you inappropriately access a patient’s record that is not part of your job duties:

- Two St. Vincent employees and one community physician plead guilty to Federal charges that they snooped in a VIP’s record. They were fired from their jobs and face high fines and possible prison time.
- Other similar cases around the country (i.e. Britney Spears, George Clooney & the “Octo” Mom)
Add slides here for

Honey, how was your day?

Picture of couple at dinner.
Social Networks Are Not Private!

• Remember that when you are communicating with someone via IM, Facebook, Twitter, etc., NONE of these things are private.

• You should *never* discuss patient care via these methods, even if you believe you have de-identified the patient information.

• Electronic Public Displays of patient information without Patient Authorization are prohibited. This includes the posting of photographs, video or any information about a UAMS patient through any electronic means including, but not limited to, social networking sites; blogs; pinning; pinging; and tweeting.
Guard PHI!
Your HIPAA Team

- Vera Chenault, UAMS HIPAA Campus Coordinator (501-603-1379)
- Anita Westbrook, Medical Center Privacy Officer (501-526-6502)
- Jennifer Sharp, Research Privacy Officer (501-686-8062)
- Steve Cochran, Security Officer (501-603-1336)
- Bill Dobbins, Informatics Manager & Auditor (501-526-7436)
- Evelyn Churchville, HR and Training Coordinator (501-603-1379)

http://www.hipaa.uams.edu