Putting HIPAA Into Practice
CUMG
May 2012

Presented by the
UAMS HIPAA Office
Yolanda Hill
Why HIPAA Matters

• HIPAA is the law, but in the end protecting patient confidentiality is how we show we care.

  99.2% of our patients - “It is important to me that members of my health team respect my privacy when I am at the hospital or clinic”
“Reasonable Safeguards” 3.1.38

• UAMS must take reasonable steps to make sure PHI is kept private
• 84% of our patients agree or strongly agree - “It is important to me that members of my health team communicate quietly with one another.”
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
Electronic PHI

• Minimize your computer screen if someone walks up
• Log off or lock your computer prior to stepping away from it
• Encrypt any email containing PHI sent outside UAMS intranet by using [Secure] in the subject line of the email
• All computers and laptops and thumb drives containing PHI must be encrypted.
Printed PHI

• When retrieving information from the printer and sending information, check every page to make sure it is the correct patient.
• Also make sure other patients’ information is not included on the page.
• Don’t leave PHI “lying around” where others can see it.
• Don’t put PHI in the regular trash. Shred or place in the privacy bins.
Printed PHI, contd.

• Don’t leave the building with PHI.
Breaches and Breach Reporting

Real Life Example

An employee of a large hospital accidentally left a scheduling sheet containing the information of 192 patients on a subway train. The records were never recovered. The hospital settled with the OCR for $1 million.
What is a Breach?

• 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. permitted by the Privacy Rule that poses a significant risk of financial reputational or other harm.

For example:
• PHI is sent to the wrong fax, mailing address or printer
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.
• If insufficient contact info for 10 or more patients, UAMS must post on our website
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 recipient’s fax number before transmittal.
• Confirm receipt of fax
• Notify your supervisor/HIPAA Office immediately if a fax is sent in error.
Social Networking

• Do not post photographs, video or any information about a UAMS patient through an electronic means such as social networking sites, blogs, pinging and tweeting.

• The only exception is a response to a UAMS patient that gives no further information about the patient. For example:

“A mom posts to your face book wall how much she appreciates you handling a billing issue. If you reply, you would not include any mention of the patients’ heath issues or even the name if she didn’t include that information in her original posting.”
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.
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.
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.
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 (501-526-7559)
- Steve Cochran, Security Officer (501-603-1336)
- Bill Dobbins, HIPAA Auditor and Educator (501-526-7436)
- Yolanda Hill, HIPAA Auditor and Educator (501-614-2098)
- Tanya Mehran, HR and Training Coordinator (501-603-1379)

http://www.hipaa.uams.edu