Safeguarding Protected Health Information for the Clinical Laboratory

Presented by the UAMS HIPAA Office
What is HIPAA? The Health Insurance Portability and Accountability Act is a federal law that protects the privacy and security of patients’ health information.

How does HIPAA affect me? UAMS requires all workforce members to sign the UAMS Confidentiality Agreement, and to work together to protect the confidentiality and security of patient, proprietary, and other confidential information.
Why it Matters

• We are committed to creating comfort, hope and healing for our patients and families...
• Can we do that if we do not respect the privacy and security of their personal information?
New HIPAA Enforcement Requirements

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

• Strict Liability fines up to $1,000,000 per occurrence

• 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.
Protected Health Information (PHI)

Identifiers that apply to patients, their families, household members and employers:

- Name
- Address (street address, city, county, zip code (more than 3 digits) or other geographic codes)
- Dates related to patient (DOB, DOS, etc.)
- Age greater than 89
- Telephone Number
- Fax Number
- E-mail addresses
- Social Security Number
- Medical Record Number
- Health Plan Beneficiary #
- Account Number
- Certificate/License Number
- Any vehicle or device serial number
- Web URL
- Internet Protocol (IP) Address
- Finger or voice prints
- Photographic images
- Any other unique identifying number, characteristic, or code (whether generally available in the public realm or not)
Protected Health Information (PHI)

- Applies to health information in all forms: written, spoken, electronic, photographic, etc.
Any access, use or disclosure of confidential information outside of your job duties is prohibited. Audits are conducted to ensure compliance with this policy.

Never share your password with anyone (this includes people working with you, for you, or under you, or IT personnel) or leave it accessible to anyone.

Do not access information except to meet needs specific to your job.

Signing the UAMS Confidentiality Agreement is a condition of employment at UAMS.
UAMS Use and Disclosure Policy

3.1.28

- **Use** is the sharing of Protected Health Information (PHI) within the UAMS community.

- **Disclosure** is releasing or providing access to PHI to anyone outside UAMS.

- Generally, you may use and disclose PHI for treatment, payment and healthcare operations (TPO) of our organization WITHOUT patient authorization. This does *not* include research.

- If the requestor is not known to you, VERIFY their identity and authority before providing PHI.
Treatment Payment and Operations (TPO): UAMS can use and disclose PHI for treatment, payment and health care operations in accordance with our policies.

- **Treatment** - Provision of healthcare by healthcare providers including coordination of care and referrals to other providers.
- **Payment** - Activities related to reimbursement and premiums such as billing, utilization review, and eligibility determinations.
- **Operations** - Examples are: training programs, accreditation, credentialing, quality improvement activities, case management, and business planning.
- **Note**: Research is not a part of TPO.
• Disclosures required by law: limited PHI may also be used or disclosed without patient authorization when *required* by law.
Examples of disclosures required by law:

- Births and deaths
- Deaths from suspicious circumstances
- Disease reporting to the Dept. of Health for specific diseases identified by statute
- Sudden Infant Death Syndrome
- Child abuse or neglect
- Abuse of the elderly, endangered or impaired adult
- **Note:** reporting of abuse of an individual who does not fall into these categories is *not* allowed without an authorization.
Examples continued:

- Intentional infliction of knife or gunshot wounds
- Reporting to registries, such as cancer or organ transplantation
- Disclosure to regulatory agencies such as CMS, FDA, licensing boards, etc.
Except for TPO or when required or permitted by law, most other uses and disclosures require patient authorization. Examples are disclosures to attorneys and life insurance companies.

The **UAMS Authorization for Release of Information Form** includes the elements of a valid authorization required by HIPAA and can be obtained from HIM (Medical Records).

Treatment cannot be withheld for refusal to sign Authorization unless the treatment is part of a research study and then research related treatment may be withheld.
Anyone processing or obtaining release of information/authorizations must ensure all of these elements are included when authorization is required. No Authorization is needed for standard treatment, payment, or operations.

The authorization must be signed by the patient or the patient’s legal representative. Examples of legal representative include the parent or legal guardian of a minor child, or the executor of an estate when the patient is deceased.
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.
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
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?
Guard PHI!
Your HIPAA Team

- Vera Chenault, UAMS HIPAA Campus Coordinator (501-526-4817)
- 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, Informatics Manager & Auditor (501-526-7436)
- Kyla Alexander, HIPAA Auditor and Educator (501-614-2098)
- Ashley Vestal, HR and Training Coordinator (501-603-1379)

http://www.hipaa.uams.edu