

Safeguarding Protected Health Information (PHI) in the Myeloma Infusion Center

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 \$1,000,000 per occurrence
- Requirement that we notify DHHS of a “breach” including inappropriate access to a patient’s record.



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
- An unencrypted laptop containing PHI is lost or stolen
- PHI is sent to the wrong fax, mailing address or printer



Exceptions

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 registration desk and in the Chemo Room.
- Try to discuss patients privately.
- Stop the conversation if someone walks up.

Leaving Messages on Answering Machines

- Limit the amount of information disclosed to the minimum necessary, such as the provider name and telephone number, or other information necessary to confirm an appointment, or to ask the individual to call back
- Do not leave messages that include test results, or other information that links a patient's name to a particular medical condition or the type of clinic or specialist
- When leaving a message with a family member or friend answering the patient's phone, the message should be limited to a request for the patient to return your call at UAMS, your name, #



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)







Your HIPAA Team

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