HIPAA: Health Insurance Portability & Accountability Act

Presented by the UAMS HIPAA Office
August 2015
HIPAA (not HIPPA)

• Is the Health Insurance Portability and Accountability Act. A federal law that protects the privacy and security of patients’ health information and grants certain rights to patients.

• How does HIPAA affect me?
  • UAMS requires all workforce members to sign the UAMS Confidentiality Agreement, as a condition of employment, 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 this be done if we do not respect the privacy and security of their personal information?
What is Protected Health Information?

- **PHI** is any individually identifiable health information transmitted or maintained that relates to:
  - past, present or future physical or mental condition
  - health care provided or
  - payment for care.
PHI Identifiers – here’s what we need to protect!

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
- 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)

• Be aware of PHI around you to avoid unintentional use or disclosure
  • Papers laying around
  • Computer screens
  • Conversations involving patients
  • Patient information on i.d. stickers, medication labels, forms
Guard PHI!

• When papers containing PHI are no longer needed, place them in a locked shred bin.
• Be careful not to leave papers at copy or fax machines, printers, or conference rooms.
• **DO NOT** take patient records off campus.
Guard PHI!

• Turn computer screens away from traffic or use privacy screens, and be aware of those around you when using PHI on computers.

• Log off or lock your computer prior to stepping away from it.
Guard PHI!

- Use private areas to discuss patient information
- Keep your voice lowered when discussing patients, and be aware of those around you
- If you overhear a conversation about a patient, keep it to yourself.
Guard PHI!

• If you do not need patient information to do your job, do not seek it out.
• Accessing patient information outside the performance of your job is a violation of UAMS policy and the law and will result in disciplinary action up to termination.
• Access to patient information is monitored and audited.
Guard PHI!

- Accessing health records for your job does not mean accessing
  - Your own record
  - The records of your family members or friends
  - The records of your co-workers
  - The records of someone in the news
Remember

• Confidentiality is a matter of respect, and is a vital component of creating comfort, hope and healing for our patients and their families.

• At some point we are all patients. Think about how you would feel if your own health information was used or disclosed in a way that was harmful to you or your family.
UAMS Policies & The Law

• UAMS HIPAA policies can be found on http://hipaa.uams.edu
• The UAMS HIPAA office can point you to the applicable policy if a question arises
• If you are unclear about a policy, please call us!
Fines and Penalties for HIPAA Violations

- Fines and criminal sanctions
  - Violations where the offender did not know they were violating the law and would have handled things differently if they did, up to $25,000/calendar year in fines.
  - Violations where the offender reasonably should have known, up to $100,000/year. Violations due to willful neglect, up to $250,000/year.
  - Violations due to willful neglect that was not corrected, up to $1.5/year.
  - Additionally, possible criminal fines up to $250,000 per violation and ten years in prison.
Fines and Penalties for HIPAA Violations

• **Concentra Health Services** has agreed to pay OCR **$1,725,220** to settle potential HIPAA violations related to a breach report that an unencrypted laptop was stolen from one of its facilities, the Springfield Missouri Physical Therapy Center.

• **A former employee of an East Texas hospital** has been **indicted for criminal violations of HIPAA** for Wrongful Disclosure of Individually Identifiable Health Information. From December 1, 2012, through January 14, 2013, the employee obtained protected health information with the intent to use the information for personal gain. If convicted, the employee could face up to ten years in prison.
UAMS Confidentiality Policy 3.1.15

• UAMS confidential information includes:
  • Protected Health Information (PHI)
  • Electronic Protected Health Information (ePHI)
  • UAMS research project information
  • Confidential employee and student information
  • UAMS proprietary information
  • Sign-on and password codes.

• The unlawful or unauthorized access, use or disclosure of confidential information is prohibited. As well as sharing or posting your password or using someone else’s password.

• Do not access information except to meet needs specific to your job.
Notice of Privacy Practices  3.1.21

• UAMS must give our patients a copy of our "Notice of Privacy Practices" which includes a description of their rights and how their health information may be used and disclosed.

• Except in emergencies, we must make a good faith effort to obtain written acknowledgement that our patients received the Notice.

• If unable to obtain acknowledgment, the attempt must be documented.

• Both English and Spanish versions may be found at: http://HIPAA.UAMS.EDU
Use and Disclosure 3.1.28

- *Use* means the sharing, employment, application, utilization, examination, or analysis within UAMS.

- *Disclosure* means the release, transfer, provision of access to, or divulging of information in any manner (verbally or in writing) by UAMS to persons who are outside of the HIPAA covered components of UAMS. Examples would be outside organizations or non-covered components of UAMS, such as the UAMS Police Department.

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

- If the requestor is not known to you, VERIFY their identity and authority before providing PHI.
TPO

• HIPAA regulations are not intended to prevent the use or disclosure of patient information for the purposes of:
  • treating the patient (anyone involved in the patient’s care can access the patient’s information)
  • obtaining payment (people involved in billing, insurance or collection of the patient’s account may access the patient’s information)
  • healthcare operations (others involved in the operations at UAMS who need the information to do their job, such as compliance staff, may access the patient’s information)

• These purposes are referred to as TPO (treatment, payment, operations) and do not require patient authorizations
Disclosures required by law

- Limited PHI may be used or disclosed without patient authorization when required or permitted by law. Examples are:
  - Communicable disease reporting
  - Suspected abuse and neglect
  - Reporting to the FDA
  - Organ donation purposes
  - To funeral directors
Authorization

• 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.

• HIPAA has several required elements for an authorization to be valid. Valid “Authorization for Release of Information” (ROI) forms may be obtained from our HIM department and on the UAMS HIPAA Office website.
Scenario

A family physician in private practice calls the UAMS Orthopedic Clinic with a request for a consultation. The UAMS Orthopedic Clinic Patient Coordinator asks for the name of the patient, the reason for the consultation request, the patient’s history, insurance information, and present medications.

The family physician will not provide any or all of this information for fear of violating HIPAA.

Would this in fact be a HIPAA violation?
Scenario

**Answer: No**, the referring physician could give this information to the orthopedic clinic without fear of violating HIPAA. Since the referral is for treatment purposes, no authorization is needed to release that information. The patient would need to sign a Notice of Privacy Practices (NPP) for the orthopedic clinic when he/she comes in for an appointment.
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 the information you need.

• For healthcare operations of UAMS such as quality improvement and teaching, de-identified information should be used when possible and the minimum necessary amount of information shared.

• Exceptions to Minimum Necessary include disclosures to or requests by a healthcare provider for treatment purposes.

Follow the simple “need to know” rule.
Patient Directory  3.1.20

- UAMS may share the following information with people who ask for the patient by name, if the patient has not opted out of the patient directory:
  - Patient Name
  - Location in our facility
  - General statement of condition (good, fair, etc.)
  - Religious affiliation (available only to clergy)
- Patients who opt out of the directory are informally referred to as “no info” patients. Before sharing any patient information with visitors, make sure the patient has not opted out of the directory.
You may share information directly relevant to the person’s involvement with the patient’s care or for payment related to care under the following circumstances:

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 the patient does not object.

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.
Safeguarding Policy 3.1.38

- UAMS must take *reasonable* steps to make sure PHI is kept private

- Permitted (with *reasonable precautions*):
  - Calling out a patient’s name in a waiting area
  - Use of a sign-in sheet containing limited information.
  - Discussing a patient’s care at nursing stations

Examples of reasonable precautions include speaking in a low voice and pulling curtains in semi-private rooms. See “HIPAA Hints” at http://hipaa.uams.edu/HIPAA_New_Materials.htm
Accidental Disclosures

• Accidental Disclosures
  • If you disclose private data in error to an unauthorized person or if you breach the security of private data, acknowledge the mistake and notify your supervisor or the HIPAA Office immediately
  • Learn from the error. Change procedures or practices, as needed and assist in correcting or recovering from the error ONLY if instructed to do so.
  • Don’t try to cover it up or “make it right” on your own.
Intentional Disclosures

• If you ignore the rules and carelessly or deliberately use or disclose Protected Health Information inappropriately, you can expect UAMS disciplinary action, civil liability, and/or criminal charges

• All intentional violations, known or suspected, must be reported immediately

  • So they can be investigated and managed
  • So a breach can be reported if necessary
  • So they can be prevented from happening again
  • So damages can be kept to a minimum
  • To minimize your personal risk
Intentional Disclosures

- Examples of intentional violations include:

  - Improper Use of Passwords can become Intentional Violations
    - Sharing, posting or distributing personal password or account access information.
    - Knowledge of unauthorized use by a co-worker of an account or password belonging to someone else.
  - Attempting to learn or use another person’s access information.
  - Improper Use of Computers can become Intentional Security Violations
    - Installing or downloading unauthorized computer programs that include or allow the entrance of viruses, worms or other malicious software.
    - Failing to secure a workstation with access to or display of confidential information.
    - Posting patient information on the Internet without authorization.
    - Placing unencrypted PHI or personal information on removable media or devices, such as thumb drives, DVD’s, and CD’s.

- Other examples of intentional violations
  - Accessing personal information outside of your job.
  - Illegally altering, destroying, or removing original paper or electronic PHI.
  - Accessing electronic PHI at home and leaving the information visible and/or accessible to family members, roommates, and friends.
  - Selling health or personal information or inappropriately giving such information to the news media.
UAMS Faxing Policy 3.1.19

- Fax machines must be in a secure location.
- **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. Make sure your name and phone number are on the fax cover sheet.
- Reconfirm recipient’s fax number before transmittal.
- Confirm receipt of fax
- **Notify your supervisor if a fax is sent to the wrong recipient.**
Patient Photography 3.1.44

- Patient consent must be obtained before photographing any part of the patient, as outlined in the Patient Photography Policy
- Do not take photographs of patients with your cell phone or personal camera
- Do not store patient photographs on any camera.
Patient Rights

HIPAA gives patients the right to:

• access, inspect and copy PHI
• request amendment of PHI
• receive accounting of disclosures
• request restrictions on disclosures
• request communications of PHI at alternative locations or means
• register complaints concerning their privacy rights.

Our toll-free contact number for privacy complaints is 1-888-511-3969 or 501-614-2187.
Patient’s Right to PHI 3.1.28

• With a few exceptions, patients can access, inspect and receive copies of their health information.

• Requests must be granted:
  • within 30 days if PHI is on-site
  • within 60 days if PHI is off-site
Amendments to PHI 3.1.32

- Patients have a right to request an amendment if they believe information in their health record is inaccurate or incomplete.

- Amendment requests should be directed to the HIM Department for processing.
Accounting of Disclosures 3.1.26

- A patient has the right to receive an accounting of PHI disclosures.

- Examples of disclosures that must be included are those required by law, such as communicable disease reporting, reporting to the Cancer Registry, and reporting to the FDA.

- All requests for Accounting should be directed to the UAMS HIPAA Office.

- Disclosures must be tracked.
Breach Reporting

• When a use or disclosure occurs that is not allowed by HIPAA, UAMS may be required to notify the patient and report the breach to the Office of Civil Rights. We may also be required to notify the media.

• All breaches must be reported to the UAMS HIPAA Office immediately.
What is a “Breach”?  

A use or disclosure of PHI that is not permitted by the Privacy Rule.  

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.
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, contact us.
HIPAA Security Rule

- **Electronic Protected Health Information (ePHI)** means individually identifiable health information that is:
  - Transmitted by electronic media
  - Maintained in electronic media
  - Received by electronic media

- The storage of ePHI is also covered under this rule.
HIPAA Security Rule

• The Security Rule covers all electronic media.

• Computer networks, desktop computers, laptop computers, personal digital assistants and handheld computers are all considered “electronic media”.

• Electronic media also includes magnetic tapes, disks, compact disks, and other means of storing electronic data (including the Internet and UAMS Intranet).
Access to ePHI

• UAMS must have policies and procedures in place to make sure that all members of the workforce have appropriate access to electronic PHI in order to perform their jobs.
• UAMS must prevent inappropriate access.
• UAMS has selected a Security Officer, Steve Cochran, who can be reached at 501-603-1336.
Security Reminders Policy

- UAMS provides all users with information, reminders, and updates on topics including:
  - UAMS information security policies
  - Significant UAMS information security controls and processes
  - Significant risks to UAMS information systems and data
  - Security best practices (e.g. how to choose a good password, how to report a security incident)
  - Reminders are often sent via email; be alert to reminders and follow directions accordingly
Password Management Policy 7.3.08

- Keep passwords confidential.

- Avoid maintaining a paper record of passwords.

- Change passwords when there is an indication of possible compromise.

- Do not use the same passwords for business and personal accounts.

- Change passwords at regular intervals (120 days) and limit reusing old passwords on domain log-on accounts.
Password Management Policy 7.3.08

- Change temporary passwords at first log-on.

- Do not include passwords in any automated log-on process, including web pages.

- Always maintain and use passwords in a secure and confidential manner.

- Password phrases or sentences are encouraged for domain log-on.
Password Management Policy 7.3.08

Passwords must:
- be based on something besides personal information so that it cannot be easily guessed or obtained

- have 8 characters and contain at least 3 of the following:
  - Capital letter
  - Lower case letter
  - Number
  - Symbol (including spaces)

- Examples:
  - #G65c1a!
  - j0ke51mn
  - The sky is blue and orange! (as a domain log-on password phrase)
Passwords

• Never 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
Security Log-In Monitoring #7.3.07

• UAMS monitors log-on attempts to the UAMS electronic information system.
• Never share passwords with others, not even IT or your supervisor.
• If you believe that someone else is inappropriately using your ID or password, immediately notify:

  Technical Support Center at 501-686-8555,
  IT Security Office at 501-686-6207 or
  ACH TechSource at 501-364-5299.
Information Access for Transfers & Terminations 3.1.41

• Department supervisors are responsible for reviewing transferring employees computer access levels and notifying the department’s IT administrator or the UAMS IT Security Office at 501-686-6207.

• Upon separation from UAMS, all employees must fill out the Employee Separation Form.
When leaving a computer unattended, lock the workstation using “control/alt/delete”, use a password protected screensaver, or log-off the computer.
Locking the computer

Press CTRL, ALT, Delete keys on the keyboard.

On the pop up window, click on the Lock Computer button.
Locking the computer

When you want to work on the computer again you will need to login with your domain password.
Information Access Management Policy 7.3.04 & Internet Policy 7.2.11

- Access to confidential information and ePHI is granted to authorized individuals on a need-to-know basis.

- UAMS computers should be used only for authorized purposes. Do not access information outside the performance of your job duties.

- Do not use computers to engage in any activity that is illegal under local, state, federal, or international law.

- Do not use workstations to engage in any activity that is in violation of UAMS policy. For example, do not access inappropriate or offensive websites, engage in gambling, send malicious emails, or download copyrighted materials.

- Never disclose or provide ePHI to others except in accordance with UAMS policies and procedures.
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.
Social Networks are NOT Private!

• UAMS policy prohibits the posting of any information about patients on websites, including Facebook and other social media sites. Violations of this policy will result in disciplinary action up to termination.
Cloud Computing

Cloud computing is never an allowed method of storing any UAMS confidential information, such as documents containing patient information. That means any services such as iCloud, DropBox or Google Docs, or forwarding documents to webmail services such as Gmail or Hotmail is never allowed.

A Business Associate Agreement is required with any company that stores UAMS PHI.
Malicious Software Policy  7.3.15

• If you detect or suspect malicious software or a virus notify the UAMS Technical Support Center 686-8555 or ACH TechSource 501-364-5299 immediately.

• Do not install personal software or download Internet software onto UAMS computers. Examples- Kazaa, Weatherbug, anti-virus software, and/or pop-up blockers onto UAMS computers.

• Downloading Internet software onto your computer may install spyware without your knowledge and cause your programs to run slower or not function properly, or create a security risk.
Facility Physical Access Controls 7.3.09

- Physical Safeguards are security measures to protect any UAMS electronic information, system hardware, and related buildings and equipment.

- For example, exterior doors should be locked appropriately at all times or have measures in place to screen visitors as they enter.
Physical Security

• PCs, mobile devices, such as PDA’s, Blackberrys, laptops, digital cameras, CD’s and diskettes, or any other devices containing confidential information or ePHI must be secured and encrypted. **It is a violation of UAMS policy to store PHI on unencrypted mobile devices and doing so will result in disciplinary action.**

• All computers, remote and on-site, that contain ePHI must be protected with a secure log-on and must be encrypted.

• Anti-virus software approved by the UAMS Information Security office must be installed on all computers that ever connect to the UAMS network (including home computers).

• **ePHI** must be destroyed before hardware or media is disposed of or made available for re-use. Contact the UAMS IT Office for information.
Working from Home 3.1.40

• If UAMS allows you to perform some or all of your work in your home, you are responsible for maintaining the privacy and security of all confidential materials.

• This includes, but is not limited to:
  • Patient Charts
  • Computers
  • Confidential Working Papers

• All UAMS confidential materials must be kept in a location that is not accessible to children, spouses, or others.

• UAMS materials must be put away when not being used.
Safeguarding PHI 3.1.38 - Using and Transporting PHI

- Confidential information, including PHI, is not to be removed from UAMS without prior approval.
- You are responsible for maintaining the privacy and security of all confidential information that you may be transporting, storing or accessing off-site.
- Check your pockets and bags at the end of the day to ensure you are not carrying patient information home.
- NEVER leave PHI in an unattended vehicle.
Access Controls for Confidential Information
7.3.14 - ePHI Transmissions

• All transmissions of ePHI and confidential information from UAMS to an outside network must utilize an encryption mechanism between the sending and receiving entities.

• Encryption makes the information “unreadable” by anyone who doesn’t have the “key”.
Highlights - UAMS E-mail Policy 7.1.12

• Remember that UAMS e-mail resources are for official UAMS business only.

• Some guidelines you should follow when e-mailing PHI and confidential information include:
  
  • When possible, only e-mail patient information within the UAMS Intranet as intranet communications are automatically encrypted.
  
  • Limit the information provided to the minimum necessary.
Highlights - UAMS E-mail Policy 7.1.12

• Guidelines (Cont’d):
  • Be careful how you “say things” in e-mails and do not e-mail extremely sensitive information.
  • Do not use e-mail as your only means to communicate information that needs immediate attention. Follow-up with a phone call or page.
  • Be cautious when forwarding any e-mails that may contain PHI or confidential information.
  • Use the encryption feature of the UAMS e-mail system when sending e-mail outside the UAMS domain.
  • Never forward to or use a personal email service (like Gmail or Yahoo) to email confidential information.
Encrypting UAMS E-mail Messages

- To encrypt e-mail sent from a UAMS e-mail account:
  - type [secure] into the subject field of the message. This method will work for both Outlook and Web mail.

For a detailed instruction guide, go to:
http://www.uams.edu/email/Instructions/Securemail/SecureMessageDeliveryInstructions.html
Other System Access

• Access to additional UAMS information systems is granted at the request of your supervisor after you complete any required training for that software. Examples may include our patient records systems, such as Epic, EPF, Sunrise, Centricity, and appointment and billing systems such as HBOC and SMS.

• Access to these systems will only be granted upon review and approval as needed for your job.
UAMS Technical Support Center

Having computer Problems?

Here’s How To Help The Technical Support Center Work For You!

• Information You Should KNOW Before You Call
  • Last Name, First name Domain login name
  • Campus location w/Room #
  • Contact Phone # or Pager
  • Problem description
  • Application &/or Operating system name
    Ex: Word 2007, Sunrise, Windows XP
  • UAMS property Tag# & computer name

UAMS Tech Support - 501-686-8555 techsupport@uams.edu
ACH Tech Source - 501-364-5299
Reporting Policy 3.1.23

• All known or suspected violations of the privacy and security regulations must be reported.
• There will be no retaliation for good faith reporting.
• Reports can be made to:
  – Reporting line at 1-888-511-3969
  – HIPAA Office 501-614-2187
  – HIPAA Inbox at HIPAA@UAMS.EDU
  – Anyone in a position of responsibility- the person receiving the report should then contact the HIPAA Office.
Your HIPAA Team

- If you have a question, concern, or problem, contact your privacy officer, the HIPAA Office, or the HIPAA hotline
Your HIPAA Team

If you have a question, concern, or problem, contact the HIPAA Office (listed below) or the HIPAA hotline (614-2187)

- Heather Schmiegelow, HIPAA Campus Coordinator  (501) 603-1379
- Anita Westbrook, Medical Ctr. Privacy Officer    (501) 526-6502
- Jennifer Holland, Research Privacy Officer       (501) 526-7559
- Tracy Petty, PRI Compliance Officer             (501) 526-8177
- Steve Cochran, Security Officer                 (501) 603-1336
- Bill Dobbins, Informatics Manager & Auditor     (501) 526-7436
- Steve DiGiovanna, HIPAA Compliance Manager      (501) 614-2098
- Brittany Parker, Education Coordinator          (501) 603-1379
More help!

*HIPAA Websites:*

UAMS HIPAA (policies and other HIPAA information)
http://hipaa.uams.edu

Department of Health and Human Services
http://www.hhs.gov/ocr/privacy/index.html

Centers for Medicaid & Medicare Services  HIPAA Web Page
http://www.cms.hhs.gov/HIPAAAGenInfo

American Medical Association
http://www.ama-assn.org