

HIPAA Privacy & Security Medical Student Orientation 2009

Presented by the UAMS HIPAA Office
Ashley Vestal

HIPAA

- HIPAA is the Health Insurance Portability and Accountability Act
- The Privacy Rule provides for the protection of patient privacy and grants patients certain rights regarding their health information
- The Security Rule provides for the security of electronically stored health information

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

Applies to health information in all forms: written, spoken, electronic, photographic, etc.

Privacy

- Protection of patient privacy is part of providing comfort, hope and healing to our patients
- Protection of patient privacy is fundamental to the practice of medicine... *“What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about.”*

Privacy

- HIPAA and UAMS policies are not intended to interfere with the treatment of patients or to restrict access to patient records for the purpose of making healthcare decisions
- This training and the staff of the UAMS HIPAA office are here to assist you in identifying ways you can protect PHI and comply with HIPAA

UAMS Confidentiality Policy 3.1.15

- 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 of PHI 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.

UAMS Use and Disclosure of PHI Policy 3.1.28

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

UAMS Use and Disclosure of PHI Policy 3.1.28

- Disclosures required by law: limited PHI may also be used or disclosed without patient authorization when *required* by law.

UAMS Use and Disclosure of PHI Policy 3.1.28

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 that reporting of abuse of an individual who does not fall into these categories is *not* allowed without an authorization

UAMS Use and Disclosure of PHI Policy 3.1.28

Examples cont.'d

- 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.

Patient Authorization

Except for TPO or when required 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 Minimum Necessary Policy 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.
- An exception to the Minimum Necessary Rule is disclosures to or requests by a healthcare provider for *treatment* purposes



UAMS Minimum Necessary Policy 3.1.25

Identify the types of information different groups of UAMS employees need to do their jobs and make reasonable efforts to limit access to only that data. That is why a registration person has different computer privileges than a nurse does. They need different information to do their jobs.



UAMS Minimum Necessary Policy 3.1.25

Require that employees access and share private patient information only on a “need-to-know” basis as part of their job duties.

In other words, you can only view information related to the job you are doing, as outlined in the **UAMS Confidentiality Agreement** you sign.

This patient information should not be shared with others who do not have the “need-to-know” inside or outside of UAMS.

Additionally, employees may not access health information such as their own health records or those of family members, when it is not part of their job duties (they may do so through proper channels).

Sharing information with Family and Friends Involved in the Patient's Care Policy 3.1.28

Generally, 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...

Sharing information with Family and Friends Involved in the Patient's Care Policy 3.1.28

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 patient does not object.

Sharing information with Family and Friends Involved in the Patient's Care Policy 3.1.28

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.

Safeguards Policy

3.1.38

UAMS must take *reasonable* steps to make sure PHI is kept private. Incidental disclosures happen when reasonable safeguards have been taken to protect a patient's information and a visitor or another patient happens to hear or see the PHI that you are using. You will not be liable for incidental disclosures, provided you are taking reasonable precautions. This section helps identify practical ways to protect PHI.

Safeguards Policy

3.1.38

- Permitted (with *reasonable precautions*):
 - Calling out a patient's name in a waiting area
 - Use of a sign-in sheet containing limited information
 - Talk about a patient's care at nursing stations
 - Treatment of patients in semi-private rooms

Safeguards Policy

3.1.38

- Examples of Safeguards
 - Do not leave PHI on unattended desks, computer terminals, fax machines, or copiers.
 - If you happen to notice PHI that is left out, don't read through it; close it, cover it, or put it away.
 - After business hours or when not in use, PHI should be supervised or kept in a locked location.
 - Avoid discussing PHI in public areas such as cafeterias and elevators.
 - Dispose of PHI properly by shredding or placing in a locked shredding bin.
 - When accessing PHI on a computer, be aware of anyone nearby and don't allow them to view your computer screen. If you are using a computer on wheels, turn it so that it faces away from heavy traffic areas like hallways.

Patient Rights

HIPAA gives patients rights to:

- access, inspect and copy PHI
 - UAMS Policy 3.1.28
- request amendment of PHI
 - UAMS Policy 3.1.32
- receive accounting of disclosures
 - UAMS Policy 3.1.26
- request restrictions on disclosures
 - UAMS Policy 3.1.34
- have communications of PHI made at alternative locations or by alternative means
 - UAMS Policy 3.1.18

Patient Rights

Exceptions to patient rights to access, inspect, and copy PHI are:

- psychotherapy notes
 - UAMS Policy 3.1.24
- information that a health care professional thinks could be harmful
- information for use in a civil or criminal trial or administrative proceeding
- certain laboratory information

Patient Rights

- Restriction requests Policy 3.1.34
 - Patients can request restrictions on the use and disclosure of PHI
 - If agreed, the provider must restrict those disclosures
 - Exceptions for emergency situations

Patient Rights

- Amendment requests
 - Processed by the Privacy Officer and HIM (medical records)
 - May be denied, if we determine that the health record is complete and accurate

Other Privacy Policies

– 3.1.37 Verification of Identity

- Verify the identity and authority of all individuals requesting Protected Health Information. If you know that a family member participates in the care of the patient, that is sufficient verification to discuss care issues.

– 14.1.01 Disclosures to Media

- All requests for publicity or interviews should be channeled through the Office of Communications and Marketing.

HIPAA and Research

– 3.1.27 HIPAA Research

- The Principal Investigator (PI) or Project Director (PD) is responsible for obtaining IRB approval for all Research projects that use human subjects including Research projects that propose the use of an individual's or Research subject's PHI.
- **Additional** HIPAA Research training is required.

Security of ePHI

- Examples of 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, thumb drives and other means of storing electronic data (including the Internet and UAMS Intranet).

Security of ePHI

Password Management

- Passwords should be:
 - a minimum length of six characters
 - based on something besides personal information so that it cannot be easily guessed or obtained
 - Composed of a mix of numeric and alphabetical characters
- Keep passwords confidential – **NEVER** share your password!!
- 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 (90 days) and limit reusing old passwords on domain log-on accounts
- Change temporary passwords at first log-on
- Do not include passwords in any automated log-on process, including web pages

Security Login Monitoring Policy 7. 3.07

Report Unauthorized Access/Use

- If you believe that someone else is inappropriately using your ID or password, immediately notify the Technical Support Center

Disciplinary Action

- **You are personally responsible for the access of any information using your password. You are in violation of UAMS policies and subject to disciplinary action if you access information that you do not need to perform your job at UAMS or allow someone else to access information using your logon information whether they are authorized to view that information or not.**

Information Access Management Policy 7.3.04 and Internet Policy 7.2.11

Computer Access

- Access to confidential information and **ePHI or other confidential information** is granted to authorized individuals on a need-to-know basis.
- UAMS computers should be used only for authorized purposes.
- Do not use computers to engage in any activity that is illegal under local, state, federal, or international law.
- Do not use computers to engage in any activity that is in violation of UAMS policy.
- Never disclose or provide ePHI or other confidential information to others except in accordance with UAMS policies and procedures.

Log-on and Access Monitoring Policy 7.3.07

- UAMS monitors log-on attempts to the UAMS electronic information systems (including the medical records systems)
- If you suspect inappropriate log-on attempts, you must report it to the IT Security Office
- You must only access UAMS information systems through your username and password.
- **All UAMS computer systems and accounts are subject to audit and your access may be monitored.**

Access Controls for Confidential Information Policy 7.3.14

Locking the Computer

- When leaving a computer unattended, lock the computer using “control/alt/delete” or log-off the computer.
- To lock the computer:
 - Press CTRL, ALT, Delete keys on the keyboard to lock the computer.
 - On the pop up window, click on the Lock Computer button.

Malicious Software Policy 7.3.15

To protect against malicious software such as “worms” and “viruses”:

- Anti-virus software is installed and kept current on all required information systems.
- Never bypass or disable anti-virus software.
- Email attachments are scanned for viruses prior to delivery. However, you should delete emails before opening when they appear suspicious, or if you do not know who sent the email.
- If you detect or suspect malicious software or a virus, notify the **UAMS Technical Support Center at 501-686-8555 or at ACH call TechSource 501-364-5299 immediately.**
- Do not install personal software or download Internet software, such as 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.

Physical Safeguards – Safeguarding PHI Policy 3.1.38

- PCs, mobile devices, such as PDAs, Blackberrys, laptops, digital cameras, CDs and diskettes, or any other devices containing **confidential** information or **ePHI or other confidential information** must be encrypted.
- All computers, remote and on-site, including home computers that contain **ePHI or other confidential information** must be protected with a secure log-on.
- All UAMS electronic media that contains ePHI or other confidential information should be marked as confidential.
- Anti-virus software approved by the UAMS Information Security office must be installed on all computers that may connect to the UAMS network. This includes your home computer.
- **ePHI or other confidential information** must be destroyed before hardware or media containing ePHI or other confidential information is disposed of or made available for re-use. Deleting the files is not sufficient to remove the information, and additional measures must be taken. Contact the Technical Support Center for information regarding this.

Mobile Device Safeguards Policy 3.1.17

- Users are required to use password protection features and automatic time-outs.
- Mobile Devices sent for outside repairs must have PHI deleted and erased from storage or a Business Associate agreement in place.
- Mobile Devices containing PHI must be stored in a secure manner to prevent access by persons who are not authorized to view the PHI stored in the device.
- **Unless absolutely necessary, Confidential Information should not be stored on mobile devices. If it is necessary to store data on mobile devices, it must be encrypted.**
- Lost or stolen Mobile Devices containing PHI must be reported to UAMS IT Security Officer (686-8555) and the UAMS Campus Police (686-7777) immediately.

Working from Home Policy 3.1.40

- **Confidentiality Extends to the Home**
 - If UAMS allows you to perform some or all of your work from 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 should be kept in a location that is not accessible to children, spouses, or other family members.
 - All possible precautions should be taken to protect confidential information from inappropriate access, loss and theft. Loss or theft of a mobile device potentially containing PHI must be reported to the Security Officer or HIPAA Office immediately.
 - UAMS materials should be put away when not being used.

Safeguarding PHI

Policy 3.1.38

Using and Transporting PHI Off-Site

- 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. UAMS policies are in effect whether you are off-site or in one of our facilities.

Access Controls for Confidential Information Policy 7.3.14

- **ePHI or other Confidential Information Transmissions – Encryption**
 - When PHI or other confidential information is sent electronically from one point to another, it must be secured to avoid theft, damage, or destruction of the information.
- **Encrypting Email – Special steps must be taken to encrypt email sent outside of UAMS if it contains ePHI or other confidential information.**
- **Email sent within the UAMS intranet is automatically encrypted.**

Accidental and Intentional Disclosures

Accidental Disclosures

- Mistakes happen...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
 - 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.

Accidental and Intentional Disclosures

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 they can be prevented from happening again
 - So damages can be kept to a minimum
 - To minimize your personal risk

HIPAA Penalties for Noncompliance

- **UAMS Disciplinary Notice Policy 4.4.02**
 - **Employee Sanctions:** Violations by UAMS workforce may result in disciplinary action, up to and including termination from employment with UAMS.
- **U. S. Government Sanctions**
 - In addition, *you* can be subject
 - to civil and criminal penalties imposed by the federal government up to \$250,000 and 10 years in prison.

UAMS has a HIPAA Team to help you!

- Vera Chenault, UAMS HIPAA Campus Coordinator (501-603-1379)
- Anita Westbrook, Medical Center Privacy Officer (501-526-6502)
- Pamela “Mo” Valentine, Research Privacy Officer (501-686-5502)
- Steve Cochran, Security Officer (501-603-1336)
- Bill Dobbins, Informatics Manager, Auditor and Educator (501-526-7436)
- Kyla Alexander, HIPAA Auditor and Educator (501-614-2098)
- Ashley Vestal, HIPAA Educator (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.dhhs.gov/ocr/hipaa/>

American Medical Association

www.ama-assn.org