“Confidentiality is everyone’s job, not everyone’s business”

February 17, 2006
Health Insurance Portability and Accountability Act (HIPAA)

This training material is designed to help educate staff members concerning HIPAA legislation, the proper use and disclosure of protected health information (PHI), the proper safeguards for confidential information including electronic protected health information (ePHI or other confidential information), and highlights from UAMS HIPAA Policies and Procedures. It is not intended to replace UAMS Policies. Please refer to the actual policy and departmental procedures and workflows for additional details.

HIPAA Education & Training Policy # 3.1.30

- All members of the UAMS workforce (employees, students, volunteers, official visitors) must receive HIPAA Training.
- In addition, your supervisor will provide specific training on policies and procedures in your work area.
- All researchers are also required to complete the online HIPAA Research Training Module at [http://www.uams.edu/orc/](http://www.uams.edu/orc/).

*NOTE: These training sessions are in addition to other department or campus training that may be required.

HIPAA – What is it?

- Health Insurance Portability and Accountability of Act 1996
- Standardizes how electronic claims are processed
- Secures systems/processes that contain Protected Health Information (PHI)
- Promotes privacy/security of individually identifiable health information (IIHI)

Health information should be protected from:

- people who aren’t involved in the patient’s direct treatment
- insurers using it to deny life or disability coverage
- employers using it in hiring/firing decisions
- reporters
- nosy neighbors, family members, or coworkers
Key HIPAA Standards and Timelines

   Imposes restrictions on the use and disclosure of protected health information (PHI) by UAMS and its employees.
   • Protects individually identifiable health information that is used/disclosed in any form-electronic, paper, or oral.
   • PHI is to be used/disclosed for health purposes only, with a few exceptions.
   • Use/disclosure of PHI is limited to minimum necessary.

   • Standard electronic formats for claims and billing.
   • Uniform codes that all insurance plans must use.
   • Rule covers defined electronic transactions. Examples include claims, enrollment, eligibility, payment and remittance advice.

3. Security - Compliance date - April 20, 2005
   Designed to ensure the security and integrity of electronically stored health information.

Definition of PHI

Protected Health Information (PHI) is any health information that may identify the patient and that relates to:
• past, present or future physical or mental health condition; or
• health care services provided; or
• payment for health care.

Examples of PHI include but are not limited to:
• patient status boards
• eligibility printouts
• financial records
• fax sheets
• test results
• data stored on internet/intranet
• data used for research purposes.
• a sign-in sheet that includes a patient’s name and reason for visit
• a patient’s identification bracelet
• an insurance card
• a detailed appointment reminder left on an answering machine.
WHEN IS PHI NO LONGER “IDENTIFIABLE?” – Policy # 3.1.31

Answer: When the “identifiers” about the patient (and the patient’s relatives, employer and household members) are removed.

A person’s identity can be discovered without knowing the person’s name. For example, a home address, or the name of a parent, or the name of the employer, or the children’s names could be used to determine a person’s identity, without any other information.

Therefore, the HIPAA Regulations provide that – until the “identifiers” about a person are removed – any health information about that person that includes even one “identifier” is PHI and is protected by HIPAA.

There are eighteen PHI identifiers, and they apply to patients, relatives, employers or household members of the patients.

<table>
<thead>
<tr>
<th>•Name</th>
<th>•Address (street address, city, county, zip code (more than 3 digits) or other geographic codes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>•Dates directly related to patient</td>
<td>•Telephone Number</td>
</tr>
<tr>
<td>•Fax Number</td>
<td>•email addresses</td>
</tr>
<tr>
<td>•Social Security Number</td>
<td>•Medical Record Number</td>
</tr>
<tr>
<td>•Health Plan Beneficiary Number</td>
<td>•Account Number</td>
</tr>
<tr>
<td>•Certificate/License Number</td>
<td>•Any vehicle or device serial number</td>
</tr>
<tr>
<td>•Web URL</td>
<td>•Internet Protocol (IP) Address</td>
</tr>
<tr>
<td>•Finger or voice prints</td>
<td>•Photographic images</td>
</tr>
<tr>
<td>•Any other unique identifying number, characteristic, or code (whether generally available in the public realm or not)</td>
<td>•Age greater than 89 (due to the 90 year old and over population is relatively small)</td>
</tr>
</tbody>
</table>
UAMS Confidentiality Policy 3.1.15

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

UAMS Confidentiality Policy highlights:
  • Unlawful or unauthorized access, use or disclosure of confidential information is prohibited.
  • Never share or post your password
  • 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 Notice of Privacy Practices Policy 3.1.21

UAMS must give our patients a copy of our "Notice of Privacy Practices" no later than the date of the first delivery of service. The Notice describes:
  • how health information may be used and disclosed
  • the patient’s rights
  • our organization’s responsibilities
  • how to file a complaint
  • who to contact for more information

Notice of Privacy Practices
  • Except in emergency situations, we must make a good faith effort to obtain written acknowledgment that our patients received the Notice.
  • If unable to obtain acknowledgment, we must document why.
  • The UAMS Notice of Privacy Practices is posted in our buildings and on our website.
  • Both English and Spanish versions may be found at: http://HIPAA.UAMS.EDU
**Scenario**

Mr. Harley comes to the UAMS Ophthalmology Clinic for treatment. This is his first visit to UAMS since the April 14, 2003 HIPAA Privacy compliance date. Mr. Harley is given the Notice of Privacy Practices (NPP) and is asked to sign the Acknowledgement.

Mr. Harley refuses to sign the Acknowledgement. The front desk clerk tells him he cannot be seen by the physician unless he signs the Acknowledgement. Mr. Harley leaves upset.

Was the statement the clerk made to Mr. Harley **True** **or** **False**?

**Answer:** False. Treatment is not withheld because the patient refused to sign the Acknowledgement. Documentation that an effort was made in good faith and that the patient refused should be noted on the acknowledgement form and included in the patient’s chart.

**UAMS Use and Disclosure Policy 3.1.28**

UAMS policies and procedures outline how protected health information (PHI) can be used and disclosed.

- **Use** is the sharing of Protected Health Information (PHI) within the UAMS community, which includes UAMS off-campus facilities such as: all AHECS, KidsFirst, and ACH.
- **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.
- 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 (TPO) as described in our Notice of Privacy Practices and 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 treatment, payment or operations

Disclosures Required by Law

Limited PHI may also 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

Authorizations

- 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).
  - Authorizations must specify data to be used/disclosed, the persons authorized to provide and receive the data, and the purpose of the use or disclosure.
  - Authorizations must include expiration date or event and be signed and dated.
  - In addition to the “core” elements above, several statements must be included regarding revocation, conditional treatment and re-disclosures.
  - 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.
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?

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.

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

Ways UAMS meets the Minimum Necessary Requirements include:

- Identifying the types of information different groups of UAMS employees need to do their jobs and making 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.
- Requiring 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.
- Developing policies and procedures that address the information we request from and provide to outside organizations.

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

The following information may be included in a Patient Directory:

- Patient Name
- Location in our facility
- General statement of condition (good, fair, etc.)
- Religious affiliation (available only to clergy)

Unless the patient tells UAMS not to, the above information may be provided to people who ask for the patient by name. We sometimes refer to patients who ask not to be included in the patient directory as "no info" patients. Examples of how the directory might be used include assisting patient visitors, floral deliveries, etc.

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

A patient’s spouse, other family member or friends may request information regarding the patient. You should refer to your department’s specific procedures/workflows to handle these requests. 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:

**If the patient is present, or otherwise available**

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.

**If the patient is not present**

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.
Patient Rights

HIPAA gives patients the right to:
- access, inspect and copy PHI
- request amendment of PHI
- receive an accounting of disclosures
- request restrictions on disclosures – Policy 3.1.34
- request communications of PHI at alternative locations or means - Policy 3.1.18
- register complaints concerning their privacy rights.

Our contact numbers for privacy complaints are:
1-888-511-3969 (toll free) or
501-614-2187 (local)

When you encounter a request related to a patient right under HIPAA you should refer to the specific policy/procedure in your area that addresses it. If you still have questions, ask your supervisor. Although the patient has the right to make these requests, UAMS is not always required to grant the request. The following are some general guidelines regarding patient’s rights.

Right to Access, inspect and receive copies of PHI Policy 3.1.28

With a few exceptions, patients can access, inspect and receive copies of their health information.
- The request must be granted:
  - within 30 days if PHI is on-site
  - within 60 days if PHI is off-site
- Exceptions include if a health care professional believes it could be harmful.
- If access to certain PHI is denied, then only the denied information may be withheld, and the rest of the information must be provided.

UAMS Amendments to PHI Policy 3.1.32

Patients have a right to request an amendment if they believe their information is inaccurate or incomplete. Examples of when the amendment request may be denied are:
- when the PHI is already accurate and complete
- when the PHI was not created by the provider, and the creator is available

Our HIM Department (Medical Records) will process amendment requests.
Scenario

A wife brings her husband to the Emergency Department of a hospital in Conway, Arkansas and says that the automobile accident that led to the injury occurred because the patient was drinking. This information is recorded in the patient’s medical record. The patient is referred to UAMS to be seen by an orthopedist. The orthopedist uses the history provided by the ER physician in Conway.

The patient files a lawsuit related to the accident and demands that the Orthopedist amend the history from the ER physician in Conway.

Should the record be amended by the Orthopedist?

Answer: No. The UAMS orthopedic physician did not originate the information. The ER physician in Conway would be the one to amend the information but he is not required to under law if he believes that original information is accurate and complete.

UAMS Accounting for Disclosures Policy 3.1.26

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

An accounting of disclosures includes:

- the date of each disclosure
- who received the PHI and their address if known
- a brief description of the PHI disclosed
- a brief statement of the purpose of the disclosure

Disclosures exempt from accounting include disclosures:

- for treatment, payment, or health care operations
- based on a patient’s signed authorization

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.

Our HIM Department will process requests for “An Accounting of Disclosures”
**Scenario**

A patient requests an accounting of disclosures. The UAMS Medical Records Department produces a list of the following:

1. a report to the State Health Department of a STD;
2. the provision of a copy of the patient’s medical record to an attorney under a written patient authorization; and
3. an instance where progress notes were provided to the patient’s PCP.

Which one of these is the one that should be included in the accounting of disclosures?

**Answer**: 1. A report to the State Health Department of a STD is the correct answer because it is required by law and does not require patient authorization. This disclosure must be included in an accounting of disclosures.

2. Disclosures do not have to be accounted for if the patient has signed an authorization for that disclosure.

3. Progress notes provided to the PCP are considered in the scope of treatment. Disclosures for treatment, payment, and operations do not require authorization and do not have to be included in an accounting.

**Privacy Rule Administrative Requirements**

The Privacy Rule requires privacy policies, procedures, and systems, such as:

- implementing “safeguards”
- selecting a Privacy Officer
- providing privacy training for the workforce
- setting sanctions for violations

**“Reasonable Safeguards”**

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.
- Talk about 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” page 27.
**UAMS Safeguard Policy 3.1.38**

- 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.

**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
- Reconfirm recipient’s fax number before transmittal
- Confirm receipt of fax
- Notify your supervisor if a fax is sent to the wrong recipient

**Business Associate Policy 3.1.33**

If UAMS provides PHI to an outside entity to perform a function for or on behalf of UAMS, HIPAA requires that we enter into a Business Associate Agreement that specifies how they will use and safeguard our patient information. Examples of our business associates are outside transcriptionists and some software vendors.

**HIPAA Research Policy 3.1.27**

Research is not considered a part of "operations" and requires a Human Subject Consent Form and HIPAA Authorization or waiver of both from the IRB.

- HIPAA permits use of de-identified data (defined as removal of 18 specific identifiers listed above) for research purposes without authorization.
- HIPAA permits use and disclosure of a limited data set (includes some of the items removed above) provided a data use agreement is obtained.
- HIPAA permits use/disclosure of PHI for research with patient authorization and IRB approval or waiver from the IRB.
As required by FDA and OHRP, individuals must sign informed consent to participate in a clinical trial.

There are special rules regarding pre-research and research on the deceased.

Contact Office of Research and Sponsored Programs for detailed guidelines regarding HIPAA and research activities.

**HIPAA Security Rule – General Requirements**

The HIPAA Security Rule compliance date is **April 20, 2005**. It requires additional protections for electronic PHI (ePHI or other confidential information).

The primary focus of the HIPAA Security Rule is to:

- Protect electronic Protected Health Information (ePHI or other confidential information) against unauthorized access, and improper alteration or destruction.
- Protect against threats or hazards to the security and integrity of ePHI or other confidential information.
- Protect against unauthorized uses or disclosures of ePHI or other confidential information.
- Make ePHI or other confidential information readily available to authorized personnel when needed.

To do this, security measures must be in place, and it is **your job** to abide by the UAMS policies to meet the HIPAA Security requirements.

**What is Electronic Protected Health Information (ePHI or other confidential information)?**

Electronic Protected Health Information (ePHI or other confidential information) is PHI created, received, stored or transmitted electronically.

Examples of ePHI or other confidential information include, but are not limited to:

- laboratory results that are emailed to a patient,
- demographic information about a patient contained in UAMS information systems such as eChart, WebChart and Logician,
- a note regarding a patient stored in your Palm Pilot,
- billing information that is saved to a CD or disk, and
• a digital photograph of a patient stored on your hard drive.

The Security Rule covers all electronic media.
• Computer networks, desktop computers, laptop computers, personal digital assistants (PDA) and handheld computers are all considered “electronic media.”
• Electronic media also includes magnetic tapes, disks, compact disks (CDs) and other means of storing electronic data. (This includes the Internet and UAMS Intranet.)

What must UAMS do?

Facility Physical Access Controls Policy 7.3.09

The Security Rule lists a wide range of activities for which UAMS must provide protection.
For example, we must safeguard:
• Computer hardware and software.
• Buildings that house computer hardware and software.
• Storage and disposal of data and the back-up of data.
• Who has access to data.
Visitor access to any facilities.

There are three categories of Security “standards:”
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

**Administrative Safeguards**

- 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 appointed a Security Officer. The UAMS Security Officer can be reached at 501-603-1336.

As a UAMS Workforce Member, your role is to be familiar with and follow these policies and procedures to protect electronic patient information. You also must take steps to make certain ePHI or other confidential information is not inappropriately seen or altered.

**Information Security and Password Management Policy 7.3.08**

**Password Management**

Choosing a good password and keeping it secure are two of the most important steps you can take to protect electronic information.

**Password Reminders**
- Keep your 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.
- Always maintain and use passwords in a secure and confidential manner.
- Password phrases or sentences are encouraged for domain log-ons.

**Selecting a strong password**

Passwords should be:
- a minimum length of six characters.
- based on something besides personal information so that they cannot be easily guessed or obtained. For example, do not use names of family members or pets.
composed of a mix of numeric and alphabetical characters.

Examples of strong passwords are:

- #G65c1
- jOke51mn
- The sky is blue and orange! (as a domain log-on password phrase)

**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 at 501-686-8555 or the Security Office at 501-686-6207. If you are an UAMS employee located at ACH or work off-campus for the Department of Pediatrics you can call TechSource at 501-364-5299.

**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.

Janie, a new employee in your clinic, has not received her log-on to the appointment system. You really need help scheduling appointments. You know that Michael, the other scheduler, keeps his password under his keyboard. What should you do?

A. Let Janie use your password to the appointment system.
B. Tell Janie you are sure Michael won't mind if she just “borrows” his password since he is off today. Show her where he keeps it.
C. Let your supervisor know so she can make sure she submitted a request for Janie a log-on to the appointment system and has scheduled her for appointment system training. Remind Michael about the proper way to store his password.

**Answer C is the correct answer.** In the interim, Janie will not be able to use the appointment system since sharing of passwords is prohibited by UAMS policy, and you and Michael will be held accountable for information accessed under your log-on. It is preferable not to write your password on paper. If you do need a written record, it must be kept in a secure location and should never be posted on or around your computer.
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 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 computers 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 or other confidential information** to others except in accordance with UAMS policies and procedures.

Your co-worker had a biopsy performed at UAMS. You are worried about her and are anxious to get the results. What should you do?

A. Check WebChart for the results.
B. Call a friend who works in pathology and ask her to get the report for you.
C. Wait for your co-worker to share her biopsy result with you.

The correct answer is C. You should wait for your co-worker to share the results with you if she chooses to do so. You should never access patient information outside the performance of your job duties, and you should not ask a “friend” to do so either. Inappropriate access to patient information can result in disciplinary action up to and including termination.

Log-on and Access Monitoring Policy 7.3.07

- UAMS monitors log-on attempts to the UAMS electronic information systems.
- **If you suspect inappropriate log-on attempts, you must report it to the IT Security Office at 501-686-6207 or the Technical Support Center at 501-686-8555 or at ACH call TechSource at 501-364-5299.** For example, if you don’t share a computer, and you notice another user signed on your computer while you were away at lunch either confirm the user had their own log-on or report appropriately.
- You must only access UAMS information systems through your username and password.
- All UAMS computer systems are subject to audit and your access may be monitored.
Information Access for Transferring and Terminating Employees Policy 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 so appropriate adjustments can be made.
- Upon separation from UAMS, all access is terminated.

Access Controls for Confidential Information Policy 7.3.14

Locked the Computer

When leaving a computer unattended, lock the computer using “control/alt/delete” or log-off the computer.

To lock the computer:
1. Press CTRL, ALT, Delete keys on the keyboard to lock the computer.
2. On the pop up window, click on the Lock Computer button.

When you want to work on the computer again, you will need to login with your domain password.
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.

Security Reminders

UAMS provides all users with information, reminders, and updates to reinforce security training and to provide additional information. Topics include:

- 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 sent via email from UAMS “Mail Administration”. Be alert to reminders and follow directions accordingly.

Physical Safeguards – Safeguarding PHI Policy 3.1.38

Physical Safeguards are security measures to protect UAMS electronic information systems 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.

- 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 should be secured.
• 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 at 501-686-8555 or at ACH TechSource at 501-364-5299.

• Destruction of UAMS Electronic Media may be accomplished in the following ways:
  – Break diskettes or otherwise render it impossible to re-insert it into a PC drive; or
  – Punch a hole through the entire diskette; or
  – Cut CDs into pieces with standard tin-snips; or
  – Request destruction of CDs and diskettes by a shredding company contracted with UAMS to destroy diskettes and CDs.
  – Hard drives and tapes are destroyed by UAMS IT Department or its designee.

**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.

• UAMS materials should be put away when not being used.

If you are assigned to work from home in an official UAMS capacity, part-time or full-time, and UAMS confidential information is involved, you must sign a formal agreement outlining how information will be safeguarded.

Contact the UAMS HIPAA Office, 501-603-1379, for agreement content specifications.
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. For example, if confidential information is involved:

- Any confidential information or ePHI or other confidential information sent from laptops, PDAs and other mobile devices must be encrypted and must be transported and stored in a secure manner. One of the most common risks with these devices is theft.
- Anti-virus software must be installed on all home computers and mobile devices used for UAMS business, and they must be password protected.
- Passwords must not be shared or accessible to family members or others.
- All media containing PHI must be disposed of appropriately and must never be placed in regular trash. This includes printed information, diskettes and CDs. (Refer to Safeguarding PHI Policy #3.1.38)

Technical Safeguards

Tracking Activity

Technical Safeguards include the use of computer technology solutions to protect electronic PHI and track activity in information systems.

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.

- Encryption makes the information “unreadable” by anyone who doesn’t have the “key”.
- All transmissions of ePHI or other confidential information from UAMS to an outside network must utilize an encryption mechanism between the sending and receiving entities; or the file, document, or folder containing ePHI or other confidential information must be encrypted before transmission.
Never use an outside mail service such as Yahoo or Hotmail for transmission of messages containing ePHI or other confidential information. The UAMS Exchange mail account must be used for any transmission of messages containing ePHI or other confidential information.

When using a home computer to transmit UAMS ePHI or other confidential information, use the UAMS Webmail or one of the VPN services provided by UAMS.

Email within the UAMS Intranet is encrypted automatically.

**Encrypting Email – Special steps must be taken to encrypt email sent outside of UAMS if it contains ePHI or other confidential information.**

- There are two ways to encrypt e-mail sent from a UAMS e-mail account:

  Typing [secure] into the ‘subject’ field of the message. This will work for both Outlook and Web mail.

  ![Secure Email](image)

  OR

  Click on the ‘Mark secure’ button in the Outlook Toolbar. This works for Outlook only and you must choose to use the standard Outlook toolbar.

  ![Mark Secure](image)

  - For a detailed instruction guide, go to [http://intranet.uams.edu/it/securemail/](http://intranet.uams.edu/it/securemail/)
  - Or Call the Technical Support Center at 686-8555 for assistance.
Emailing ePHI or other confidential information Policy  7.1.12

Remember that UAMS email resources are for official UAMS business purposes only. Guidelines you should follow when emailing PHI include:

- When possible, only email patient information within the UAMS Intranet as intranet communications are automatically encrypted.
- Limit the information provided to the minimum necessary. (Refer to UAMS Minimum Necessary Policy #3.1.25.
- 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 emails that may contain PHI.
- If you email PHI outside of the UAMS intranet, you must abide by the UAMS Email Policy #7.1.12.
- Be sure and use the encryption feature of the UAMS e-mail system when sending e-mail outside the UAMS domain.

Domain Log-on & Email

When can I expect to get my domain logon account and email?

- 3 to 5 days after you turn in a signed Confidentiality Agreement. Both should be ready at same time.
- Your domain name is lastnamefirstnamemiddleinitial.
- Your initial password is your social security number, and it must be changed at first login. You must make this change from a computer on the campus network. It cannot be changed through the Internet.

What will my email address be?

- 1st Initial 2nd Initial Last name. absmith@uams.edu
- 1st Initial Last name (if you don’t have a middle initial). pduncan@uams.edu

NOTE: Students should refer to the student handbook for information concerning domain logon accounts and email.

What about access to other systems that I need to do my job?
Access to additional UAMS information systems is granted at the request of your supervisor after you complete any required training for that system. Examples may include our patient records systems, such as EPF, eChart, Logician, and appointment and billing systems such as HBOC and SMS.
**UAMS Technical Support Center**

The UAMS Technical Support Center (formerly known as the “Help Desk”) is available 24 hours a day, 7 days a week to assist you with computer/software related questions and problems. You can reach the Technical Support Center by:

- calling 501-686-8555 or
- emailing them at techsupport@uams.edu (Tech Support Center in the UAMS Address Book) or
- going to their website at [http://techsupport.uams.edu/](http://techsupport.uams.edu/)

You should have the following information available when you contact them:

- Last Name, First name, Domain login name
- Campus location with Room #
- Contact Phone # or Pager
- Problem description
- Application &/or Operating system name, for example: Word2003, eChart, Windows 2000 or XP
- UAMS property Tag# & computer name

**ACH TechSource**

UAMS employees located at ACH or working for the Department of Pediatrics off-campus should call TechSource at 501-364-5299.

ACH TechSource is available 24 hours a day, 7 days a week to assist you with computer/software related questions and problems. You can reach them by:

- calling 501-364-5299 or
- emailing them at techsource@uams.edu

You should have the following information available when you contact them:

- Last Name, First name, Domain login name
- Campus location with Room #
- Contact Phone # or Pager
- Problem description
- Application &/or Operating system name, for example: Word2003, eChart, Windows 2000 or XP
- UAMS property Tag# & computer name
UAMS Reporting Policy 3.1.23

- All known or suspected violations of the HIPAA regulations must be reported.
- There will be no retaliation for reporting of suspected violations.
- Reports by members of the workforce can be made to:
  - Reporting line at 1-888-511-3969
  - HIPAA Office 501-614-2187
  - IT Security Office 501-686-6207
  - Anyone in a position of responsibility - The person receiving the report should then contact the HIPAA Office.
- Patients and others can use the general complaint process or contact the UAMS HIPAA Office directly.
- It is important that suspected violations be reported, so we can attempt to mitigate any harmful effects and prevent the problem from happening again.

Our HIPAA Officers are:
- UAMS HIPAA Officer is Deanna Brown (501-614-2187)
- UAMS Medical Center Privacy Officer is Anita Westbrook (501-526-6502)
- UAMS Research Privacy Officer is Tim Atkinson (501-686-5502)
- UAMS Security Officer is Steve Cochran (501-603-1336)

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

Severe civil and criminal penalties: 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.

Conclusion

- We must all remember to protect the privacy and security of patient information at all times.
- We are all patients ourselves from time to time. Think about how you would feel if your own health information were used or disclosed in a way that was harmful to you or your family.
- If you have a question about HIPAA, ask your supervisor or manager, or contact your UAMS Privacy or Security Officers.
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

HIPAAAdvisory
www.hipaadvisory.com
HIPAA HINTS

“Confidentiality Is Everyone’s Job, Not Everyone’s Business”

1. Use private areas to discuss patient information, if possible.
2. Keep the volume of your voice lowered when having conversations concerning patients in non-private areas.
3. When papers containing patient information are no longer needed or required, either shred them or place in a secure shredding bin.
4. **Before talking with a patient’s family members or friends** about a patient’s condition, check with the patient first, or in the patient’s absence, information limited to the family member/friend’s involvement in the patient’s care may be shared if you can infer from the circumstances that the patient does not object, such as when the family member/friend has been present with the patient on recent visits and patient has agreed, or not objected to, their presence during your conversations with the patient.
5. **Before releasing patient information by phone**, verify caller’s identity – even if it is the patient calling. If it is not the patient, then you must verify that person’s identity and authority to have the information, or ask that the patient call instead. For example, the family member/friend situation may apply as discussed above in 4.
6. If you do not need patient information to do your job, do not seek it out. Only access/use patient information when needed to **perform your job**.
7. Log off your computer or “lock” your workstation using Ctrl/Alt/Del when you will be away from your work area, so PHI cannot be viewed or accessed in your absence.
8. Do not share your password with anyone.
9. Check the patient directory before releasing any information, including releasing patient’s room number, to see if patient opted out of directory.
10. Be careful not to leave patient information at copy machines, fax machines, printers or in conference rooms.
11. When faxing information, use an “official” UAMS coversheet and confirm recipient’s fax number and receipt of fax.
12. Medical records should not be taken off the premises.
13. Use privacy screens on computer monitors, or if one is not available, turn monitor so that it cannot be viewed by unauthorized persons passing by.
14. If you overhear a conversation concerning a patient, keep it to yourself.
15. Do not leave messages concerning a patient’s condition or test results on any answering machine.
16. Report suspected privacy violations to the HIPAA Compliance Office by calling **(501) 614-2187**.

[http://hipaa.uams.edu](http://hipaa.uams.edu)


UAMS CONFIDENTIALITY POLICY

Confidential Information includes information concerning UAMS research projects, confidential employee information, information concerning the UAMS research programs, proprietary information of UAMS, and sign-on and password codes for access to UAMS computer systems. Confidential information shall include Protected Health Information.

Protected Health Information (PHI) means information that is part of an individual’s health information that identifies the individual or there is a reasonable basis to believe the information could be used to identify the individual, including demographic information, and that (i) relates to the past, present or future physical or mental health or condition of the individual; (ii) relates to the provision of health care services to the individual; or (iii) relates to the past, present, or future payment for the provision of health care services to an individual. This includes PHI which is recorded or transmitted in any form or medium (verbally, or in writing, or electronically). PHI excludes health information maintained in educational records covered by the federal Family Educational Rights Privacy Act and health information about UAMS employees maintained by UAMS in its role as an employer.

POLICY: UAMS prohibits the unlawful or unauthorized access, use or disclosure of confidential and proprietary information obtained during the course of employment or other relationship with UAMS. As a condition of employment, continued employment or relationship with UAMS, UAMS workforce shall be required to sign the UAMS Confidentiality Agreement approved by the UAMS Office of General Counsel. UAMS will provide training for each of its workforce members on the importance of maintaining confidentiality and the specific requirements of state and federal law, including the HIPAA Privacy Regulations and laws protecting the privacy of students and employees. This policy applies to information maintained or transmitted in any form, including verbally, in writing, or in any electronic form.

PROCEDURES:

1. Confidentiality Agreement: As a condition of employment, continued employment, or a relationship with UAMS, UAMS will require such individuals to sign the UAMS Confidentiality Agreement approved by the UAMS Office of General Counsel. The Confidentiality Agreement shall include an agreement that the signing party will abide by the UAMS policies and procedures and with federal and state laws, governing the confidentiality and privacy of information.

All new employees, students, or vendors requiring access to electronic Confidential Information (computer systems) must have a current Confidentiality Agreement on file in the IT Security Office. The UAMS IT Security Office will maintain signed Confidentiality Agreements and furnish a copy to the individual signing the agreement. It is the responsibility of the manager hiring individual vendors or consultants or receiving sales representatives or service technicians (who do not require electronic access but who may have access to Confidential Information) to require execution of the appropriate confidentiality agreements approved by the UAMS Office of General Counsel and to send those documents to the UAMS IT Security Office.

2. Restriction on Access, Use and Disclosure of Confidential Information: UAMS limits and restricts access to Confidential Information and computer systems containing Confidential Information based upon the specific duties and functions of the individual seeking or requiring access. UAMS will restrict access to Confidential Information to the minimum necessary to perform individual job functions or duties. UAMS will further limit and control access to its computer systems with the use of sign-on and password codes issued by the IT Security Office to the individual user authorized to have such access.

Authorization to access, use or disclose Protected Health Information also is governed by the UAMS Use and Disclosure Policy.

UAMS will control and monitor access to Confidential Information through management oversight, identification and authentication procedures, and internal audits. UAMS managers and heads of departments will have the responsibility of educating their respective staff members about this Policy and the restrictions on the access, use and disclosure of Confidential Information, and will monitor compliance with this Policy.

3. Sales Representatives and Service Technicians: Must register in the appropriate area (Refer to UAMS Guidelines for Vendors and Sales Representatives Policy), sign and complete the Confidentiality Agreement prior to any exposure to UAMS Confidential Information.

4. Media: All contacts from the media regarding any Confidential Information must be referred to the UAMS Office of Communications and Marketing (501-686-8998 or pager 501-395-5989)

5. Violation of Confidentiality Policy: Individuals shall not access, use, or disclose Confidential Information in violation of the law or contrary to UAMS policies. Each individual allowed by UAMS to have access to Confidential Information must maintain and protect against the unauthorized access, use or disclosure of Confidential Information. Any access, use or disclosure of Confidential Information in any form – verbal, written, or electronic – which is inconsistent with or in violation of this Policy may result in disciplinary action, including but not limited to, immediate termination of employment, dismissal from an academic program, loss of privileges, or termination of relationship with UAMS.

All UAMS employees and others subject to this Policy must report any known or suspected incidents of access, use or disclosure of Confidential Information in violation of this Policy or in violation of the law.
CONFIDENTIALITY AGREEMENT

As a condition of my employment, continued employment or relationship with UAMS, I agree to abide by the requirements of the UAMS Confidentiality Policy and with federal and state laws governing confidentiality of a patient’s Protected Health Information, and I agree to the terms of this Confidentiality Agreement.

I understand and agree that if I access, use or disclose Confidential Information in any form – verbal, written, or electronic – in a manner that is inconsistent with or in violation of the Confidentiality Policy, UAMS may impose disciplinary action, including but not limited to, immediate termination of employment, dismissal from an academic program, loss of privileges, or termination of relationship with UAMS.

I understand that when I receive a sign-on code to access the UAMS Network and Systems, I have agreed to the following terms and conditions:

- The sign-on and password codes assigned to me are equivalent to my signature, and I will not share the passwords with anyone.
- I will be responsible for any use or misuse of my network or application system sign-on codes.
- I will not attempt to access information on the UAMS Network and Systems except to meet needs specific to my job or position at UAMS.

I acknowledge that I have read the terms of this Confidentiality Agreement, and that I have received a copy.

_________________________________________ SS#

(Signature)

Print Full Name: __________________________________________________________

Date: ___________________ Department: _________________________________

Witness at UAMS Orientation only, otherwise not required: ______________________

Supervisor/Manager’s Signature: ___________________________ Date: __________

(If Vendor, then Department Head Signature required)

Department Head Signature: ___________________________ Date: __________

(Please return completed form to UAMS IT Security Office, #802)
1. **Examples of Individually Identifiable Health Information that could be used to identify an individual include:**
   a. Name, License number, photograph
   b. Birth date, address, account number
   c. County, fingerprint, phone number
   d. All of the above

2. **The term Protected Health Information (PHI) includes:**
   a. Oral information about a patient
   b. Written information about a patient
   c. Individually identifiable information about a patient
   d. All of the above

3. **Compliance with HIPAA is voluntary, not mandatory.**
   a. True
   b. False

4. **I can share information about a patient if I know them personally.**
   a. True
   b. False

5. **The term HIPAA means:**
   a. Health Is Patient Access and Accountability
   b. Health Insurance Portability and Accountability Act
   c. Neither A or B

6. **Patients have the right to obtain a copy of their own records**
   a. True
   b. False

7. **Notice of Privacy Practices include:**
   a. How we use and disclose PHI
   b. The patient’s rights
   c. UAMS legal duty with respect to PHI
   d. All of the above

8. **An example of safeguarding patients PHI is:**
   a. Sharing passwords with coworkers
   b. Avoiding discussing patient’s information when others may hear you.
   c. Leaving computer screens unlocked at all times
9. Logging onto the Network and allowing someone else to use the computer is against UAMS Policy.
   a. True
   b. False

10. Which is the best way to protect sensitive data in your computer when you go out for lunch or home for the evening?
   a. Turn your monitor off
   b. Activate the screen saver
   c. Lock your computer
   d. Close all programs

11. Identify examples of computer safety:
   a. Creating alphanumeric passwords
   b. Locking computer screens while away
   c. Logging off computer at the end of workday
   d. All of the above

12. Which of the following is an example of a strong password?
   a. Steve
   b. My dog’s name
   c. #G6cZ
   d. My last name spelled backwards
   e. *j0ke5lmn

13. Other than yourself, who else should know your password?
   a. Only your supervisor, major professor, or system administrator
   b. Coworker
   c. No one

14. When a computer virus is detected, infected, or suspected it must be reported to the UAMS Information Security Office within what time frame?
   a. Immediately
   b. Never
   c. Within 24 hours

15. Of the following choices, which indicates when it is safe to open a file attached to e-mail?
   a. When you know the sender, the attachment is expected, and it is not unusual in anyway
   b. When the email is only sent to you
   c. When you know the sender
HIPAA PRIVACY and SECURITY TRAINING ACKNOWLEDGMENT

This is to acknowledge that I have completed the Required UAMS HIPAA Privacy and Security Awareness Training.

Complete the Review and Training Acknowledgement.
Send to UAMS HIPAA OFFICE, # 829