

**NUMBER: 3.1.38**

**DATE: 10/1/2003**

**REVISION: 9/19/2007; 8/18/2010**

**PAGE: 1 of 10**

---

**SECTION: ADMINISTRATION**

**AREA: GENERAL ADMINISTRATION**

**SUBJECT: SAFEGUARDING PROTECTED HEALTH INFORMATION**

---

### **PURPOSE**

To inform the UAMS Workforce on the required procedures for safeguarding Protected Health Information (PHI).

### **SCOPE**

UAMS Workforce

### **DEFINITIONS**

**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.

**Electronic Media** means:

- (1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as CD-ROM, DVD, floppy disks, magnetic tape or disk, optical disk, digital memory cards and flash drives; or
- (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

**Electronic Protected Health Information (ePHI)** means individually identifiable health information that is:

- Transmitted by Electronic media
- Maintained in Electronic media
- Received by Electronic Media

**Information System** means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

**Pre-Research or Review Preparatory to Research** means the review of information or records prior to obtaining patient authorization and consent or prior to obtaining an IRB Waiver of Authorization in which the review is solely to prepare a research protocol, to determine if a research project is feasible, or for similar purposes preparatory to research.

**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.

**UAMS Workforce** means for purposes of this Policy, physicians, employees, volunteers, trainees, and other persons whose conduct, in the performance of work for UAMS, is under the direct control of UAMS, whether or not they are paid by UAMS.

For additional definitions:

<http://hipaa.uams.edu/DEFINITIONS%20-%20HIPAA.pdf>

## **POLICY**

UAMS Workforce members must undertake appropriate administrative, technical and physical safeguards, to the extent reasonably practicable, to preclude Protected Health Information (PHI) from intentional or unintentional use or disclosure in violation of the HIPAA regulations.

Electronic Protected Health Information (ePHI) and other confidential information located on UAMS Information Systems or Electronic Media must be protected against damage, theft, and unauthorized access. This includes all ePHI and confidential information received, created, maintained and transmitted by UAMS. Confidential information must be consistently protected and managed through its entire life cycle, from origination to destruction. Controls must be in place for hardware and Electronic Media moving into, out of, and within UAMS. Information Systems and Electronic Media for which this policy applies include, but are not limited to, computers (both desktop and laptop), floppy disks, backup tapes, CD-ROMs, DVDs, zip drives, portable hard drives, digital memory cards, flash drives, hard drives in copiers and medical equipment, and PDAs.

## **PROCEDURE**

While access to PHI, and conversations regarding a patient, often must occur freely and quickly in treatment settings, the following safeguards should take place to the extent reasonably practicable:

## **1. Protecting Printed Information:**

- A. Route incoming written correspondence through the smallest number of viewers possible.
- B. Pre-address all envelopes to individuals or specific departments within UAMS.
- C. Keep printing and photocopying of documents containing PHI to a minimum.
- D. When retrieving documents from a printer, ensure that only the intended documents are taken. When printing to a shared printer, if a document containing PHI has been removed from the printer by someone else, investigate and attempt to retrieve the document.
- E. Any documents containing PHI should be placed with identifying information face down on counters, desks, and other places where patients or visitors might see them. These documents should not be left out on desks or countertops after business hours and should be placed in locked storage bins, locked desk drawers, or other secure areas.
- F. When discarding any papers containing PHI, use a shredder or place the records and items in a bin specifically designated as a shredding bin where the records and items will be retrieved for shredding. All shredding bins must be locked unless HIPAA Office approval has been obtained to keep the bin unlocked.
- G. Place shredder machines in a convenient location. If a personal shredder is used instead of a shredder serviced by UAMS's vendor, it must be a "cross-cut" shredder.
- H. When paper documents are in transit from location to location, place the documents in sleeves, bags, or envelopes that are sealed and clearly addressed to the recipient.
- I. When transporting medical records, they should never be left unattended and records should be covered or turned over so that PHI is not visible to casual observers.
- J. IV bags and other medically related material that is not suitable for shredding and is placed in regular trash should have all patient identifiers removed or obliterated.
- K. Locate fax machines in non-public areas. Refer to UAMS [\*Faxing of PHI and Other Confidential Information Policy, 3.1.19.\*](#) for additional requirements for faxing PHI.

## **2. Bulletin Boards:**

- A. Bulletin boards located in areas that may be seen by patients or visitors should not contain any documents containing PHI, unless the patient has agreed to the display by written or documented verbal permission. This would include baby pictures, cards and notes of appreciation and children's signed art work.

### **3. Storage of Paper-Based Data:**

- A. After business hours or when not in use by authorized personnel, documents or items containing PHI should be supervised or kept in a locked desk, locked cabinet or other locked location. Storage of documents containing PHI, whether on-site or off-site, must be locked at all times except during use by authorized personnel.
- B. Limit the number of keys given to employees. Provide keys to areas and locked cabinets to only those employees whose job responsibilities require or necessitate access to the areas or cabinets where PHI is stored or located.
- C. Limit access to filing areas and off-site storage facilities where records or items containing PHI are located to only those employees whose job responsibilities require access to such areas.

### **4. Physical Security:**

- A. All persons (patients, visitors, vendors and others) who are not authorized to have access to PHI should be supervised, escorted or observed when visiting or walking through an area where PHI may be easily viewed or accessed.
- B. Utilize a system of controlling the distribution of keys. Require all employees to return all keys upon the effective date of termination of their employment with UAMS, or when the job responsibilities of the employee no longer require access to the areas or cabinets accessed by the key or keys.
- C. Doors should be locked at night, unless authorized personnel need access to the rooms or areas after hours.
- D. Access to areas containing PHI should be monitored and controlled to the extent possible.

### **5. Conversations:**

- A. Conversations with a patient and other conversations in which PHI is being discussed, over the phone or in person, should be made, to the extent possible, in a manner or in a location (or both) where persons who are not intended to be a part of the conversation or who are not authorized to receive the PHI cannot easily overhear the conversation.
- B. When having a conversation in a public area with a patient, the patient's family members, or other conversations in which PHI is discussed, conduct the conversation in a lowered voice, to the extent possible, so that unauthorized persons cannot easily overhear the conversation.
- C. Avoid using patients' names or the names of patients' family members or other patient identifiers in public hallways and elevators when persons who are not authorized to receive the information are present.

- D. In an emergency situation, where a patient is hearing impaired or in other situations where the ability to discuss PHI quietly and in private may not be practicable, take reasonable precautions to preclude the disclosure of PHI to the extent possible.

## **6. Vocera Communications**

- A. If you are using Vocera to call someone regarding a patient, let them know by saying “I need to talk to you about a patient” or something similar. Then, give the person a chance to respond before you say anything else.
- B. If you answer your Vocera in a public location such as an elevator, the cafeteria, or a patient room, let the caller know you are in a public place.
- C. When discussing a patient, keep patient identifiers and other sensitive information to the minimum necessary to accomplish your purpose

## **7. Paging:**

- A. Overhead paging of patients and patients’ family members should be kept to a minimum. Only request the page if it is urgent and you are unable to locate the patient or family by other means.
- B. Only the minimum amount of information should be used when paging. For example, “Mr. John Jones, please return to surgery waiting room.”
- C. Do not request overhead pages for patients who have asked to be omitted from the patient directory.

## **8. X-Ray Lightboards, Nursing Station Whiteboards, and Patient Tracker Boards:**

- A. Place all X-ray lightboards and nursing station whiteboards in an area generally not accessible by the public or readily visible to the public, or implement other safeguards which reasonably limit incidental disclosures to the general public.
- B. Patient tracker boards containing PHI should be limited to locations where the benefit of having the tracker board outweighs the potential risk to patient privacy. Boards must contain only the minimum information necessary for their intended purpose and should be placed in such a way as to minimize visibility to patients and visitors.

## **9. Sign-In Sheets:**

- A. Information on patient sign-in sheets should only include the patient’s name and appointment date and time. Do not include unnecessary information such as patient complaint, date of birth, or other information that is not necessary for the sign-in sheet. Use of peel-off labels for patient’s to sign, which are then transferred to a sign-in sheet

kept outside the view of other patients, is preferable to a sign-in sheet in view of other patients.

#### **10. Charts in Chart Holders Outside Exam Room:**

- A. When placing patient records in chart holders outside of examination rooms, turn the records with the front cover facing the wall or with identifying information otherwise covered, so the patient's information is not visible to passersby.

#### **11. Voice Mail/Answering Machine Messages:**

- A. When leaving a voice mail or answering machine message for a patient, always limit the amount of information disclosed to the minimum necessary, such as the provider name and telephone number, or other information necessary to confirm an appointment, or to ask the individual to call back. For example, when confirming an appointment, the information should be limited to appointment date and time, the doctor's name, and a contact name and telephone number.
- B. Do not leave messages that include laboratory and test results, or any other information that links a patient's name to a particular medical condition or the type of clinic or specialist the patient is seeing. (For example, "I am calling to remind Mrs. Brown of her chemotherapy treatment tomorrow at 10:00," is not an appropriate message.)
- C. Generally, when leaving a message with a family member or friend answering the patient's phone, the message should be limited to a request for the patient to return your call; and you may leave your name, telephone number, and the fact that you work at UAMS.
- D. A patient's verbal permission or written authorization is NOT needed in these circumstances when leaving a message for the patient as directed by this policy and procedure.

#### **12. E-Mail:**

- A. All external email messages must include a confidentiality statement, regardless of whether the email message contains PHI. PHI should not be emailed unless necessary, and care should be taken that only the intended recipients are included on the email. Email containing PHI should never be sent to a user group unless the sender is certain of every recipient and their authority to receive the information.
- B. E-mail is encrypted automatically inside the UAMS network. Any e-mails sent outside of the UAMS network containing Confidential Information, including ePHI, must be encrypted. Refer to UAMS [\*E-Mail Access and Usage Policy, 7.1.12.\*](#)

### **13. Social Networking:**

- A. Electronic Public Displays of patient information without Patient Authorization are prohibited. This includes the posting of photographs, video or any information about a UAMS patient through electronic means including, but not limited to, social networking sites; blogs; pinning; ping; and tweeting. The only exception is a posting in response to a UAMS patient that gives no further information about the patient.

### **14. Faxing:**

- A. For documents containing PHI that are faxed internally or outside UAMS, please refer to the UAMS [\*Faxing Protected Health Information or Other Confidential Information Policy, 3.1.19.\*](#)

### **15. Safeguarding ePHI and other Confidential Information in Electronic Format:**

- A. Access to ePHI through UAMS's clinical systems is through user authentication and password.
- B. Access to Information Systems and Electronic Media containing ePHI and other confidential information at UAMS must be provided only to authorized UAMS workforce members who have a need for specific access in order to accomplish their job duties. UAMS workforce members must not attempt to access, duplicate or transmit Electronic Media containing ePHI and other confidential information for which they do not have appropriate authorization. Refer to [\*Information Access Management Policy, 7.3.04\*](#) and [\*Confidentiality Policy, 3.1.15.\*](#)
- C. User access may require specific training depending on the system before access is allowed.
- D. PHI should not be stored on Electronic Storage Media such as, CDs, thumb drives, diskettes and DVDs unless absolutely necessary, and then only the minimum necessary for the shortest time necessary. All electronic storage media containing PHI must be encrypted when possible and must be marked as confidential. [\*Refer to Policy 3.1.17, Mobile Device Safeguards.\*](#)
- E. UAMS Information Systems and Electronic Media containing ePHI or other Confidential Information should be located and stored in secure environments that are protected by appropriate security barriers and entry controls.
- F. UAMS Information Systems and Electronic Media containing ePHI and other confidential information must be disposed of properly when no longer needed.
  - a. Electronic Media containing ePHI or other Confidential Information that is to be disposed of permanently must be physically destroyed, and may be accomplished in one of the following ways:

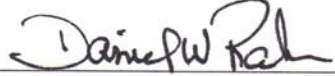
1. Break diskettes or otherwise render it impossible to re-insert it into a PC drive
  2. Punch a hole through the entire diskette
  3. Cut CDs/DVDs into pieces with standard tin-snips
  4. Request destruction of CDs/DVDs and diskettes by a shredding company contracted with UAMS to destroy diskettes and CDs
  5. Data on flash drives must be securely deleted using an appropriate method. Contact UAMS IT for assistance with this.
  6. Hard drives and tapes are to be destroyed by UAMS IT Department or its designee. Contact UAMS Technical Support with questions regarding disposal.
- b. Disposal of UAMS Information Systems and equipment containing ePHI must be tracked and logged. At a minimum, such tracking and logging must provide the following information:
1. Date of disposal
  2. Who performed the disposal
  3. Brief description of media or Information Systems that was disposed
- c. ePHI should be removed from equipment or Information Systems that are being returned to the vendor. If that is not possible, a Business Associate Agreement must be in place before the equipment is returned to the vendor. Contact UAMS Office of Contract Services for more information about Business Associate Agreements.
- G. ePHI on UAMS Electronic Media must be removed before such electronic media can be re-used.
- H. UAMS Workforce members moving UAMS Information Systems and Electronic Media containing Confidential Information, including ePHI, into, out of, and within the workplace must maintain records of such movement.
- I. When necessary, a retrievable, exact copy of data will be created before equipment is moved.
- J. ePHI and other confidential information used or sent for Review Preparatory to Research may not be removed from UAMS. Refer to [HIPAA Research Policy 3.1.27.](#)
- K. ePHI and other confidential information used or sent outside the UAMS Network should be encrypted.
- 16. Transporting and/or Accessing UAMS Confidential Information off campus for official business use.**
- A. Confidential Information, including PHI, is not to be removed from UAMS by members of the Workforce without prior approval and a signed confidentiality agreement on file.

For employees who work from home part-time or full-time in an official UAMS Capacity refer also to UAMS Administrative Guide [Working from Home Policy 3.1.40.](#)

- B. The Workforce member is responsible for maintaining the privacy and security of all Confidential Information that they may be transporting, storing or accessing off-site. This includes, but is not limited to:
  - a. Protected Health Information and Electronic Protected Health Information
  - b. Computers or mobile devices that contain or access Confidential Information.
  - c. Storage media such as diskettes, CD-ROMs, DVDs, digital memory cards, and flash drives containing Confidential Information.
  - d. Printed documents that contain Confidential Information.
  
- C. UAMS policies are in effect whether the Workforce member is working off-site or in a UAMS facility and include the following requirements:
  - a. Electronic media and printed information must be transported and stored in a secure manner.
  - b. The printing of confidential information from home computers should be kept to a minimum and only as needed in accordance with UAMS policies.
  - c. All media containing PHI or ePHI must be disposed of appropriately and must never be placed in regular trash. This includes printed information, faxes, hard drives, diskettes and CDs.
  - d. UAMS materials must be put away when not being used and kept in a secure location that is not accessible to others including children, spouse and visitors.
  - e. Passwords must not be shared or accessible to family members or others
  - f. Any Confidential Information or ePHI sent from workstations, laptops, PDAs and other mobile devices must be encrypted. Refer to [Mobile Device Safeguards Policy 3.1.17.](#)
  - g. Anti-virus software must be installed on all home computers and mobile devices used for UAMS business, and they must be password protected.
  - h. Employees are required to maintain updates to current operating systems (ex. Microsoft updates/patches)
  - i. Confidential Information must not be saved on local hard drives or other media except when necessary to perform UAMS job duties. All saved Confidential Information must be encrypted and deleted when no longer needed. Confidential Information including PHI must not be saved on public workstations such as in hotels and libraries.
  - j. When away from the UAMS network, the use of web based applications to access ePHI such as WebChart and WebEPF should be minimized. When it is necessary to use resources outside of the UAMS network to access web based applications such as WebChart, be sure to delete Cookies, delete files and clear the history in your Browser.

**SANCTIONS**

Violation of this Policy will result in disciplinary action, in accordance with [Policy 4.4.02](#).

Signature: 

Date: February 24, 2011