

HIPAA Highlights for UAMS Cancer Registry

Excerpts from Safeguarding PHI Policy 3.1.38

7. Conversations:

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.

- A. 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.
- B. Avoid using patients' names or the names of patients' family members in public hallways and elevators when persons who are not authorized to receive the information are present.
- C. 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.

12. 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.

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.
- D. 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.

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. 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).
- Developing policies and procedures that address the information we request from and provide to outside organizations.

Follow the simple “need to know” rule

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 (both internal and external faxes)
- Reconfirm recipient's fax number before transmittal
- Confirm receipt of fax
- Notify your supervisor if a fax is sent to the wrong recipient

Passwords

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.

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 (at least 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 must be:

- a minimum length of eight 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.
- Must have **8** characters and contain at least **3** of the following:
 - Capital letter
 - Lower case letter
 - Number
 - Symbol (including spaces)
 - Examples:
 - I am UAMS.
 - I hate passwords!
 - Simple4U

Locking 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.