

HIPAA Audits of Access to Protected Health Information (PHI)

Why are HIPAA audits performed?

As part of UAMS' compliance with the HIPAA Privacy and Security Rules, access to patient records must be monitored to help make certain that Protected Health Information (PHI) is used and disclosed appropriately, and that PHI is not accessed outside the performance of your specific job duties. Part of this monitoring process includes the UAMS HIPAA Office performing audits of access to patient records.

Why would the UAMS HIPAA Office Call Me?

The auditors obtain a report of who accessed a specific patient's record. If your name is on the report, and the appropriateness is not readily apparent to the auditors, you or your supervisor will be contacted to verify that this access falls within your job duties. This is routine follow-up and is done for physicians, students and staff members where there are questions regarding why he or she was in a patient's record.

Access of patient records outside the performance of your job is prohibited

It is against UAMS policy for physicians, employees and students to access patient information outside the performance of their job duties. In other words, you must not look at, print, copy, or share information regarding any UAMS patient who is not under your care or a part of your job performance/workload. This includes your own records and the records of:

- Family
- Friends and acquaintances
- Colleagues, co-workers and fellow students

For example, if you are a UAMS provider, it would be within your job duties to access a record if you are the treating physician, have been asked by another UAMS physician to consult on the patient, or are asked by clinic staff for assistance in the absence of the patient's physician. However, it would not be appropriate for you to review a colleague's or other UAMS employee's records if you are not directly involved in their care, even if they are a patient in your clinic.

What should you do?

Follow the **"need to know"** rule. Before accessing patient information, ask yourself "Do I need to know this information to perform my job duties"? If the answer is "no", don't access the information.

Audits and the disciplinary process

When you sign the UAMS Confidentiality Agreement, you agree, "not to attempt to access information on the UAMS network and systems except to meet needs specific to my job or position at UAMS." Violations of the Confidentiality Policy and other UAMS HIPAA Policies are taken so seriously that your supervisor will be notified and must impose disciplinary action. The Employee Disciplinary Notice policy allows your supervisor to proceed directly to a written warning or termination of employment depending on the circumstances.

Some of the "safeguards" required of you by UAMS policy when using UAMS Information Systems include:

1. Never share your password.
2. Always use your own unique sign-on and password when accessing confidential information.
3. 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 accessed in your absence.
4. Do not access confidential information, including PHI, outside the performance of your job duties.

Helpful Links to UAMS HIPAA training and information: <http://hipaa.uams.edu/>

Sharing Information with Spouse, Family and Friends Involved in Patient's Care

Excerpted from UAMS Policy 3.1.28--Use and Disclosure of Protected Health Information

SECTION 6 – DISCLOSURES TO SPOUSE/FAMILY/FRIENDS INVOLVED IN PATIENT'S CARE – No Patient Authorization, but Special Circumstances Must Exist.

1. **Verification of Identity:** The identity of the patient and the person receiving the PHI must be verified. In making verification decisions in these *particular* circumstances, UAMS may rely on the exercise of professional judgment of its staff to determine a person's identity.
2. **When Patient Present (in person or on phone): Can disclose to Spouse, Family or Friends only under the following circumstances:**
 - A. If the spouse, family or friend is identified by the patient; and
 - B. The spouse, family or friend is involved in the patient's care; and
 - C. One of the following circumstances exists:
 - a. Patient has agreed (verbally on phone or otherwise); or
 - b. Patient does not object when provided opportunity to do so; or
 - c. You can reasonably infer from circumstances that the patient does not object (such as when patient brings family member into examination room); or
 - d. There is a medical emergency.

PHI disclosed in these circumstances must be limited to PHI that is directly relevant to person's involvement with the patient's care or payment; **or** to notify them of patient's location, one word statement of general condition, or death.

3. **When Patient is NOT Present (in person or on phone), then we may:**
 - A. Disclose (by phone or otherwise) to spouse/family/friends involved in patient's care PHI that is directly relevant to the person's involvement with the individual's health care or payment if we determine that disclosure is in the best interest of the patient.
 - B. Allow person to pick up filled prescriptions, medical supplies, X-rays or other similar forms of PHI, using professional judgment and experience with common practice to make reasonable inferences of the patient's best interest in allowing a person to act on behalf of the individual.
4. **When Patient Cannot Agree/Object Because of Patient's Incapacity or an Emergency Circumstance, then we may:**
 - A. Disclose [by phone or otherwise] the PHI permitted for the facility directory (name, location and one word statement of general condition), but only if this is consistent with a prior expressed preference of the patient and it is in the patient's best interest to do; and
 - B. Disclose [by phone or otherwise] to spouse/family/friends involved in patient's care PHI that is directly relevant to the person's involvement with the individual's health care or payment if we determine that disclosure is in the best interest of the patient; and

Allow person to pick up filled prescriptions, medical supplies, X-rays or other similar forms of PHI, using professional judgment and experience with common practice to make reasonable inferences of the patient's best interest in allowing a person to act on behalf of the individual.

The full text of the use and disclosure policy is located at:
http://uams.edu/AdminGuide/PDFs/hipaa_3.1.28.pdf

Some Helpful Tips for Proper Handling and Disposal of PHI

GENERAL CONSIDERATIONS-

- Place documents with identifying information **face down or protect with a cover** if they contain PHI and must be maintained on counters, desks or other places where patients or visitors might see them.
- Keep documents in locked storage bins, locked desk drawers, or other secure areas after business hours
- Be careful not to leave patient information at copy machines, fax machines, printers or in conference rooms.
- **DO NOT dispose of PHI in the trash or recycling bin.** When discarding records or items containing PHI, use a shredder or place in a locked bin specifically designated as a shredding bin where the PHI will remain secure. All shredding bins are to remain locked.
- **IV bags and other medically related materials not suitable for shredding** that are placed in a regular trash container should have all patient identifiers removed or obliterated. White labels (Central supply # 92352) are in the Omnicels for this particular use. Be sure that when you discard an IV bag with the patient's name on it in the regular trash, that you cover all PHI, including the name and account number, with the white label before discarding.

ROUNDING- It is always best for clinicians to discuss patient care in the physician workspace or an empty office. Observe the following precautions to safeguard PHI while Rounding:

- When rounding in the halls or discussing a patient's treatment at the nursing stations, keep the volume of your voice lowered so visitors do not overhear details of a patient's care and treatment.
- The "Wallaroos" offer a convenient way to store the bedside chart and for clinicians to review a chart outside the room prior to conferring with the patient. Do not leave charts open on Wallaroos and keep Wallaroos closed when not in use. If your visit with the patient is complete, return the patient chart to the nurses' desk.
- Do not leave patient information unattended. When charts are not in use at the nursing station, close them and return to the chart rack or shelf.
- Log off computers when you are finished so that patient information will not be viewed or accessed on unattended workstations.
- When using the Computers on Wheels (COWs), minimize the screen if a visitor walks up.
- When conferring with a patient in a semi private room, close the curtain prior to discussing care, and lower your voice to minimize the ability of the other patient to overhear the discussion. If there are visitors in the room, you should ask them to leave while you are conferring with the patient, unless the patient requests the visitor remain in the room.
- Before talking with a patient's family members or friends about a patient's condition, check with the patient first.