HIPAA Hints

HIPAA Audits Monitor Access to Protected Health Information

By Bill Dobbins, HIPAA Compliance Audit Manager

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 the records of a colleague or other UAMS employee's records if you are not directly involved in their care, even if they are 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. In addition to any discipline by UAMS, if a determination is made that the inappropriate access constitutes a reportable breach under the HIPAA rules, we are required by law to notify the patient and report it to the Office of Civil Rights.

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'll be away from your work area so PHI can't be accessed in your absence.
4. Do not access confidential information, including PHI, outside the performance of your job duties.

For helpful links to UAMS HIPAA training and information, visit: **http://hipaa.uams.edu**.