



UAMS

HIPAA HYPE

**"Confidentiality is everyone's job,
not everyone's business"**

September 2003

It's September and we made it past the big HIPAA Privacy implementation hurdle! So what's really different now? As healthcare providers, we've always respected and protected patients' health information. The difference is that now we have a federal regulation that tells us how our patients' information must be handled. Not only that, we have to tell our patients what their rights are regarding their PHI. Our policies must clearly state how we will do this.

If you have an idea for improving workflows while maintaining our compliance with the HIPAA Privacy Rule, please let us know! Your suggestions are welcome and may be sent to us in several ways:

1. E-mail us at HIPAA@UAMS.EDU
2. Interoffice Mail to #829
3. Phone calls to 603-1379

The initial HIPAA training effort has been quite successful and we appreciate your efforts to learn what it takes to help our patients – and our co-workers! – learn about these new standards and procedures. HIPAA training will be an on-going process for us at UAMS. Most new employees will receive their training at orientation. Current employees should expect to see newsletters, e-mails, posters, etc., updating them on policies and procedures.

Here's a list of the HIPAA-specific policies for your convenience. They may be accessed by going to HIPAA.UAMS.EDU and clicking on policies and procedures, or by going to the UAMS Intranet and looking them up in the Admin Guide.

Here's a short quiz based on the HIPAA Hints on the following page.

1. Passwords should be kept on the front of your monitor.
True
False
2. Medical records can be taken off campus if locked in the trunk of your car.
True
False
3. All patients at UAMS should receive a copy of our Notice of Privacy Practices
True
False
4. The elevator is a good place for an update on a patient's condition.
True
False

Policy No.	HIPAA Specific and Related Policies
3.1.26	Accounting for Disclosures
3.1.33	Business Associate Policy
7.3.03	Computer Device Custodial Practices
3.1.15	Confidentiality Policy
3.1.31	De-Identification of PHI
14.1.01	Disclosures to the Media
3.1.19	Faxing Policy and Form
3.1.30	HIPAA Education and Training
3.1.25	Minimum Necessary
3.1.22	Mitigation of Uses/Disclosures in Violation of HIPAA
3.1.21	Notice of Privacy Practices Policy
3.1.34	Patient Information Restriction Requests
3.1.32	Patient's Request to Amend Medical Records/PHI
3.1.17	Personal Digital Assistants (PDA) Safeguards
3.1.24	Psychotherapy Notes
3.1.20	Release of Patient Directory Information
3.1.18	Request for Alternative Method of Communications of PHI
3.1.29	Requests for Data Extracts
3.1.23	Reporting Policy for HIPAA Violations
3.1.27	HIPAA Research Policy
3.1.28	Use and Disclosures of PHI and Medical Records
3.1.35	Use of PHI for Fundraising
3.1.36	Use of PHI for Marketing
3.1.37	Verification of Identity

Those policies in bold above, should be reviewed by all employees. All others should be reviewed as needed in your according to your duties. You should speak with your supervisor about which policies apply to you.

1. Do not discuss patient information in cafeteria lines, in elevators or when others who do not need to know can hear.
2. Use private areas to discuss patient information, if possible.
3. Keep the volume of your voice lowered when having conversations concerning patients in non-private areas.
4. Place all non-needed papers containing patient information in a shredding bin or other secure container.
5. Before talking with family members or friends about a patient's condition, check with the patient.
6. When releasing patient information by phone, verify caller's identity.
7. Avoid leaving patient information out in view of others.
8. If you do not need patient information to do your job, do not seek it out.
9. Only use patient information when needed to perform your job.
10. Log off your computer when you will be away from your work area if you have accessed patient information.
11. Do not share your password with anyone.
12. Check the patient directory before releasing any information, including room numbers, to see if patient opted out of directory.
13. Be careful not to leave patient information at copy machines, fax machines, printers or in conference rooms.
14. Remove patient diagnosis information from white boards.
15. Medical records should not be taken off the UAMS campus.
16. Surgery schedules that contain PHI should not be left out in view of others or placed in trash, but should be placed in shredding bins.
17. 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 your work area.
18. Hand out the UAMS Notice of Privacy Practices.
19. If you overhear a conversation concerning a patient, keep it to yourself.
20. Do not leave messages concerning a patient's condition or test results on any answering machine.
- 21. Report suspected privacy violations to the HIPAA Compliance Officer by calling 614-2187.**