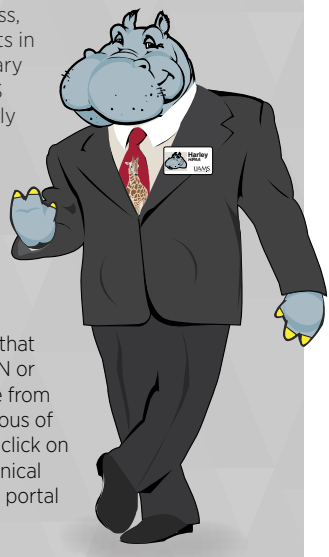
HIPAA HINTS

HIPAA is a federal law that protects the privacy of patients' health information. UAMS requires all workforce members to sign the UAMS Confidentiality Agreement, and to work together to protect the confidentiality and security of patient information and other confidential information. For helpful information, go to the HIPAA website at http://hipaa.uams.edu or call the HIPAA office at (501) 614-2187.

1. Use private areas to discuss patient information, if possible.
2. Keep the volume of your voice lowered when having conversations concerning patients in non- private areas. If you overhear a conversation concerning a patient, keep it to yourself.
3. When papers containing patient information are no longer needed or required, either shred them or place in a secure shredding bin. DO NOT dispose of paper PHI in a waste basket.
4. Before talking with a patient's family members or friends about a patient's condition, it is best practice to check with the patient first.
5. Before releasing patient information by phone, verify caller's identity – even if it is the patient calling. If it is not the patient, then you must verify that person's identity and authority to have the information, or ask that the patient call instead. For example, the family member/friend situation may apply as discussed above in 4.
6. Only access/use patient information when needed to perform your specific job duties
7. Log off your computer or "lock" your workstation using Ctrl/Alt/Del when you will be away from your work area so that PHI cannot be viewed or accessed in your absence.
8. Do not share your password with anyone or leave it where someone might see it. Never use the logon credentials of another user.
9. Check to make sure the encounter is not marked private before releasing any information, *including the patient's room number, if a visitor calls inquiring about a patient.*
10. Be careful not to leave patient information at copy machines, fax machines, printers or in conference rooms.
11. When faxing information internally or externally, use an "official" UAMS coversheet and confirm recipient's fax number and receipt of fax.
12. If necessary to remove patient information from UAMS premises, be sure to follow the appropriate UAMS policies and procedures.
13. When emailing patient information to a non-UAMS email address, make sure the email is encrypted by typing [secure] in brackets in the subject line. Limit the information to the minimum necessary to accomplish the intended purpose. Emails sent from a UAMS email address to another UAMS email address are automatically encrypted and secure.
14. Store patient information only on mobile devices (thumb drives and laptops) that are encrypted.
15. Use privacy screens on computer monitors, or if one is not available, turn monitor or computer on wheels so that it cannot be viewed by unauthorized persons passing by.
16. Do not leave messages concerning a patient's condition or test results on any answering machine.
17. Protect yourself against phishing attacks. Be cautious of emails that request sensitive information such as your log in credentials, SSN or bank account number. Be suspicious of emails that appear to be from someone at UAMS who does not normally email you. Be suspicious of emails instructing you to open an attachment or instruct you to click on a hyperlink. Report suspected phishing attacks to UAMS IT Technical Support Center at (501-686-8555) or through the IT self-service portal at http://itss.uams.edu.



Policy No.	HIPAA-Specific and Related Policies
2.1.11	Accounting of Disclosures of PHI
2.1.39	Audit Controls for Confidential Information
2.1.29	Authorized Remote Use of Confidential Information
2.1.18	Business Associate Policy
2.1.34	Computer Device Custodial Practices to Protect Confidential Information
2.1.27	Confidential Shred Bin Usage
2.1.01	Confidentiality Policy
2.1.16	De-Identification of Protected Health Information and Limited Data Set Information
2.1.41	Disaster Recovery
13.1.02	Disclosures to the Media
2.1.31	Email Access and Usage
2.1.40	Enterprise Data Integrity & Encryption
2.1.38	Facility Physical Access Controls
2.1.04	Faxing of Protected Health Information or Other Confidential Information
2.1.33	Generic Accounts
2.1.15	HIPAA Education and Training
2.1.12	HIPAA Research Policy
2.1.42	HIPAA Sanctions Policy
2.1.25	Identity Theft Protection
2.1.30	Information Access for Transfers and Terminations
2.1.35	Information Access Management
2.1.37	Information Security & Password Management
2.1.36	IT Risk Analysis and Risk Management of Electronic Systems
2.1.32	IT Security Incident Identification and Handling Policy
2.1.24	Job Shadowing
2.1.10	Minimum Necessary Policy
2.1.07	Mitigation of Uses/Disclosures in Violation of HIPAA
2.1.02	Mobile Device Safeguards
2.1.06	Notice of Privacy Practices
2.1.19	Patient Information Restriction Requests
2.1.26	Patient Photography, Audio Recording, Videography, and Other Imaging
2.1.17	Patient's Request to Amend Medical Records or PHI
2.1.28	Protected Health Information Breach Notification and Reporting
2.1.09	Psychotherapy Notes Policy
2.1.05	Release of Patient Directory Information
2.1.08	Reporting of HIPAA Violations
2.1.03	Request for Alternative Method of Communications of Protected Health Information
2.1.14	Request for Data Extracts
2.1.23	Safeguarding Protected Health Information
2.1.20	Use and Disclosure of PHI for Fundraising
2.1.13	Use and Disclosure of PHI and Medical Records Policy
2.1.21	Use of PHI for Marketing
2.1.22	Verification of Identity and Authority to Receive PHI

http://hipaa.uams.edu

"Confidentiality is a team sport;
when we protect PHI, everyone wins"

UAMS