



HIPAA HINTS

What is HIPAA? The Health Insurance Portability and Accountability Act is a federal law that protects the privacy of patients' health information.

How does HIPAA affect me? UAMS requires all workforce members to sign the UAMS Confidentiality Agreement, and to work together to protect the confidentiality and security of

patient, proprietary, and other confidential information. A list of UAMS Privacy and Security Policies, as well as other helpful information, is available on the HIPAA website at <http://hipaa.uams.edu>.

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.
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, check with the patient first. Or in the patient's absence, information limited to the family member/friend's involvement in the patient's care may be shared if you can infer from the circumstances that the patient does not object, such as when the family member/friend has been present with the patient on recent visits and the patient has agreed, or not objected to, their presence during your conversations with the patient.
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 job and always go through the proper procedures. This includes information that you may have a right to access through other means, such as your own health information or that of your family members with their permission.
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 the patient directory before releasing any information, including the patient's room number, to see if patient opted out of directory.
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. Do not remove health information from the premises, by taking medical records, emailing patient information to a non-UAMS email address, storing patient information on flash drives or laptops, or other means, unless it is necessary and you are authorized to do so by a manager. In those cases, ensure that you take precautions, so the information does not fall into the wrong hands. Remember that any patient information copied to portable devices or media must be encrypted.
13. 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.
14. If you overhear a conversation concerning a patient, keep it to yourself.
15. Do not leave messages concerning a patient's condition or test results on any answering machine.
16. If you have any questions or concerns, call the HIPAA office at (501) 614-2187.

Policy No.**HIPAA-Specific and Related Policies**

7.3.14	Access Controls for Confidential Information
3.1.26	Accounting for Disclosures
7.3.11	Audit Controls for Confidential Information
3.1.33	Business Associate Policy
7.3.03	Computer Device Custodial Practices
3.1.15	Confidentiality Policy
3.1.39	Creation or Revision of HIPAA Policies
7.3.12	Data Integrity
3.1.31	De-Identification of PHI
7.3.13	Disaster Recovery
14.1.01	Disclosures to the Media
7.3.09	Facility Physical Access Controls
3.1.19	Faxing Policy and Form
7.3.02	Generic Accounts
3.1.30	HIPAA Education and Training
3.1.27	HIPAA Research Policy
3.1.41	Information Access for Transfers and Termination
7.3.04	Information Access Management
7.3.08	Information Security Password Management
7.3.05	Information System Activity Review
7.3.06	IT Risk Analysis and Risk Management of Systems
7.3.15	Malicious Software
3.1.25	Minimum Necessary
3.1.22	Mitigation of Uses/Disclosures in Violation of HIPAA
3.1.17	Mobile Device Safeguards
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
3.1.24	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
3.1.38	Safeguarding Protected Health Information
7.3.01	Security Incident Identification and Handling
7.3.07	Security Log In Monitoring
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
3.1.40	Working From Home

<http://hipaa.uams.edu>



**“Confidentiality is a team sport;
when we protect PHI, everyone wins”**