UAMS Reference Guide to HIPAA Policies in the Administrative Guide

Revised March, 2016

This guide is designed to be used as an overview. Supervisors must make certain that their employees are familiar with detailed policies applicable to their specific job duties. The policies are available on the UAMS Intranet at http://hipaa.uams.edu/
HIPAA Definitions can be found at http://hipaa.uams.edu/DEFINITIONS%20-%20HIPAA.pdf

Knowledge of a violation or suspected violation of these policies must be reported. The HIPAA Office phone number is 501-603-1379 and the reporting line is 1-501-614-2187.
Violation of these policies will result in disciplinary action, up to and including termination. See HIPAA Sanctions Policy 2.1.42 for more information on disciplinary actions for violations of HIPAA and UAMS policies and procedures,

Adm. Guide No.	UAMS Administrative Guide Policy Name	Policy Highlights
HIPAA PRIVACY AND SECURITY POLICIES		
2.1.11	Accounting of Disclosures of PHI	Patients may request a record of certain disclosures of their PHI that UAMS released to outside entities. There is a disclosure form, and HIM processes the request. Some disclosures are exempt from the accounting. For example: ▪ Disclosures for treatment, payment and operations ▪ Disclosures permitted by a signed patient authorization ▪ Disclosures to the patient and to individuals involved in their care Examples that must be included in the accounting are: ▪ Disclosures to AR Department of Health ▪ FDA Reporting ▪ Reporting of Abuse and Neglect ▪ Reports to the Coroner or Law Enforcement ▪ Research related disclosures without patient authorization ▪ The above is only a partial list. If you make any disclosures outside UAMS, refer to this policy and determine if the disclosures are subject to Accounting. If so, you must fill out a special form for each disclosure or enter it into "UAMS Release and Disclosure" Software System.
2.1.39	Audit Controls for Confidential Information Additional resources: UAMS Administrative Guide 2.1.08 *Reporting HIPAA Violations*	▪ Systems that contain Confidential Information will be audited. ▪ Audits may include the examination of access of certain data, software programs and utilities, use of a privileged accounts, information system start up or stop, and failed authentication attempts.
2.1.29	Authorized Remote Use of Confidential Information	▪ Members of the UAMS Workforce who are assigned to work from home part-time or full-time in an official UAMS capacity are responsible for maintaining the privacy and security of all UAMS Confidential Information including PHI & ePHI. ▪ Confidential Information, including PHI, is not to be removed from UAMS by members of the Workforce without prior approval and a signed Confidentiality Agreement on file. ▪ Confidential information includes but is not limited to: 1. Protected Health Information and Electronic Protected Health Information 2. Computers that contain or access Confidential Information 3. Confidential Working Papers ▪ UAMS policies are in effect whether the Workforce member is working off-site or in a UAMS facility. The following must be acknowledged: 2.1.01 Confidentiality Policy 2.1.23 Safeguarding PHI Policy 2.1.37 Information Security and Password Management 2.1.02 Mobile Device Safeguards

2.1.18	Business Associate Policy	▪ Business Associates perform a function or service for or on behalf of UAMS involving the use or disclosure of PHI (or vice versa, making UAMS the Business Associate). ▪ Examples are outside transcriptionists, vendors providing billing and collection services, and accrediting organizations. ▪ A Business Associate Agreement that contains specific assurances must be executed with these entities before disclosing any PHI to them. ▪ Only certain parties at UAMS are authorized to sign Business Associate Agreements. Contact UAMS Office of Contract Services, 501-686-8451.
2.1.34	Computer Device Custodial Practices to Protect Confidential Information	To protect confidential information: ▪ Workstation placement will be evaluated and monitored. ▪ Software systems containing PHI are required to have automatic logoffs at established time intervals. ▪ Signed Confidentiality Agreements are required for computer access. ▪ Access to workstations is granted to authorized individuals on a need-to-know basis. Access will be deactivated promptly for persons leaving the employ of UAMS. ▪ Department supervisors are responsible for reviewing transferring employees' computer access levels. ▪ Employees are required to safeguard Confidential Information and access it only to the extent required for official UAMS purposes. ▪ All employees and students receive information security training at time of orientation. ▪ Individuals must attend system training, as required, for use of any system containing PHI. ▪ PC's, mobile devices and any other device containing Confidential Information should be secure. ▪ Confidential information generated at UAMS is UAMS property and is not to be removed without prior approval. Users are responsible for permanently removing all UAMS Confidential Information and UAMS software from personally owned devices upon termination from UAMS.
2.1.27	Confidential Shred Bin Usage	Please refer to this policy regarding guidelines of shredding confidential information.
2.1.01	Confidentiality Policy Note: This policy is reviewed in New Employee Orientation. All employees must sign that they have received and read the policy and sign the Confidentiality Agreement.	▪ Unlawful or unauthorized access, use, or disclosure of confidential and proprietary information is prohibited. ▪ Signing the UAMS Confidentiality Agreement is a condition of employment or relationship with UAMS. ▪ Confidential Information must be protected. ▪ Passwords must never be shared. ▪ Employees may not access patient information except to meet needs specific to their job/position.
2.1.16	De-Identification of PHI and Limited Data Set Information	For PHI to be considered de-identified, the following identifiers of the patient or of relatives, employers or household members must be removed: 1) Name 2) Geographic subdivisions smaller than a state 3) All elements of dates except year 4) Telephone and Fax numbers 5) E-Mail, IP, and URL addresses 6) Social Security Number 7) Medical Record Number 8) Health Plan Beneficiary Number 9) Account Numbers 10) Certificate/license Numbers 11) Vehicle Identifiers and Serial Numbers 12) Device Identifiers & Serial Numbers 13) Biometric Identifiers, including finger and voice prints 14) Full Face or other comparable photographic images 15) Any other unique identifying number, characteristic, or code ▪ After removing the above identifiers, the information cannot be released if UAMS has actual knowledge that the information used alone or in combination with other information could identify and individual. ▪ Refer to actual policy for definition of a "Limited Data Set" and circumstances where a Limited Data Set can be released without patient authorization.
2.1.41	Disaster Recovery Additional resources: Disaster Recovery Plan Web link http://disasterrecovery.uams.edu.	▪ IT Management is responsible for establishing, implementing and maintaining the IT Disaster Recovery Plan (DRP). ▪ For network file servers, the Network Administrator is responsible for the backups and other measures necessary for the overall security of the software and data stored on the network storage. ▪ For stand-alone microcomputers, the primary user of that system is responsible for backups and any other measures necessary to insure the security and integrity of the data and software.

		▪ Individual workstation users on the network are responsible for backups and data security for local storage space. A Business Continuity Plan (BCP) is comprised of departmental procedures supplied to IT for publishing in the Disaster Recovery Plan and will serve as a guide to UAMS staff toward continuing normal business operations during an IT Emergency.
13.1.02	Disclosures to the Media	▪ Visits from the Media or requests for information from the Media are to be coordinated through the UAMS Office of Communications and Marketing. ▪ Only designated individuals in the UAMS Office of Communications and Marketing, Hospital Administration or Nursing Administration are authorized to release to the press any information concerning patients and their condition. ▪ Patient information, including acknowledgment of their presence here, will not be disclosed if the patient has opted out of the directory. If the patient has not opted out of the directory and the media asks for the patient by name, only a one-word description of the patient's condition may be released unless the patient has otherwise asked us not to, or UAMS has elected not to release information on the patient. ▪ No information regarding the death of a patient will be released prior to the notification of next-of-kin or other legal representative. ▪ Any additional release of information beyond the one-word statement of condition shall be confined to that of a general nature and requires written Authorization from the patient or the patient's legal representative.
2.1.31	E-mail and Access Usage	▪ The UAMS e-mail system is available to authorized users for the purpose of conducting UAMS business. ▪ Any e-mails sent outside of the UAMS network containing Confidential Information, including ePHI must be encrypted. Instructions on how to encrypt an e-mail are provided in the policy. 1) The patient's e-mail address is part of the patient's PHI and must be protected. 2) PHI is subject to the minimum necessary requirement of HIPAA. 3) Do not use e-mail to send highly sensitive information. 4) Confirm the e-mail address before sending Confidential Information or ePHI. 5) Caution should be used when distributing lists or forwarding e-mails that contain Confidential Information or ePHI. 6) UAMS e-mail may not be auto-forwarded to any non-UAMS account. 7) Non-UAMS email services must never be used by workforce members to communicate PHI. ▪ Prohibited Uses: Monetary gain, Sending copies in violation of copyright laws, Opening another individual's e-mail, Using e-mail to harass, intimidate or interfere with others ability to conduct business, Using e-mail for any purpose restricted or prohibited by state, federal or UAMS Policies, Spoofing—constructing an e-mail so that it appears to be from someone else, Attempting unauthorized access to e-mail or attempting to breach security measures or to intercept e-mails without proper authorization, Broadcasting e-mails to "Everyone" without prior permission, Using custom backgrounds, special formats or colors within your e-mail and Use of quotations or sayings within your message or signature block. ▪ Provider communications with patients via e-mail is left to the discretion of the physician or clinic and it is the responsibility of the clinic to determine additional e-mail communication guidelines. ▪ UAMS access and disclosure of communications—UAMS reserves the right to access and disclose the contents of faculty, staff, students and other users' e-mail without the consent of the user.
2.1.40	Enterprise Data Integrity and Encryption	• Authentication measures are implemented to protect the Integrity of Confidential Information, including ePHI, and to protect against improper and unauthorized alteration or destruction. ▪ Encryption methods must be used for all devices that manage any Confidential Information including ePHI.
2.1.38	Facility Physical Access Controls	UAMS must create and maintain appropriate access controls to limit physical access to its electronic Information Systems that contain Confidential Information, including (ePHI), and the facility or facilities in which they are housed, while ensuring properly authorized access is allowed. The following procedures must be included: 1. Allowance of physical facility access during emergencies to support restoration of data under the UAMS Emergency Response Plan (ERP). 2. Procedures to safeguard all facilities, systems, and equipment used to store Confidential Information, including ePHI, against unauthorized physical access, tampering, and theft. Examples include, but are not limited to, physical barriers, utilizing locks, alarms and other access control devices, and providing controls to guard against fire damage, power outages, and other similar occurrences. 3. Procedures to control and validate a person's access to facilities based on their role or function, including visitor control and control of access to software programs for testing and revision.

		• The UAMS Physical Plant and UAMS Police Department will maintain records of repairs and modifications performed by their respective departments to areas housing Confidential Information, including ePHI. All other areas will implement procedures to document repairs and modifications to the physical security components of their facility that house Confidential Information including locks, doors, and other physical access control hardware.
2.1.04	Faxing of PHI or Other Confidential Information	▪ Fax machines that transmit PHI and other confidential information must be in non-public, secure locations. ▪ Confidential data should be faxed only when mailing or other delivery methods will not suffice. ▪ Both internal and external faxes containing PHI and other confidential information must have a cover sheet that includes the UAMS Fax Confidentiality Statement and approved UAMS logo. ▪ The recipient's fax number should be reconfirmed before transmittal. ▪ Confirm delivery of fax by phone or by review of appropriate fax transmittal log sheet. ▪ The HIPAA Office must be contacted if a fax is sent to the wrong recipient. Contact the recipient and ask them to secure the document until further notice. • Faxed information should be stored and disposed of appropriately.
2.1.33	Generic Accounts	▪ Confidential Information must never be stored onto a system using a generic account ▪ Generic accounts will be utilized by UAMS in cases where multiple users must access one workstation to perform given duties. ▪ Generic Accounts will not require users to sign in and out of Microsoft Windows and will allow unrestricted access to Intranet resources & non-patient applications and products as needed. ▪ Requests for generic accounts areas will be reviewed and approved or disapproved as appropriate by the IT Security office. ▪ Generic Accounts will be audited on a regular schedule for appropriateness of access and ongoing need. ▪ All Patient Health Information Applications installed on generic workstations will be accessed through non-generic, individually password protected logons. Audit trails are required on all patient information systems & the audit logs will be reviewed on a regular schedule.
2.1.15	HIPAA Education and Training	All members of UAMS workforce must receive HIPAA training. HIPAA training completed by these individuals will be recorded in the UAMS Training Tracker System or other electronic training system as may be authorized by UAMS or manually maintained by the office assigned to the specific training. ▪ All physicians, fellows and residents must complete Required HIPAA Privacy and Security Training within 60 days of their appointment. ▪ All Employees attending New Employee Orientation will receive HIPAA training at that time and sign an attestation establishing that the training is completed. ▪ All other employees not attending Orientation must complete the online Required HIPAA Privacy and Security Training. ▪ All UAMS students will receive Required HIPAA Privacy and Security Training as a part of Orientation. ▪ All UAMS Volunteers will receive Required HIPAA Privacy and Security Training through the appropriate Office of Volunteers and approved by the UAMS HIPAA Office. ▪ All UAMS Official Visitors will receive Required HIPAA Privacy and Security. The UAMS Sponsor of the Visitor will provide HIPAA training materials and obtain a signed UAMS Confidentiality Agreement from the visitor. ▪ For all other persons, including affiliate students, refer to the HIPAA Training Matrix (Appendix A). ▪ Supervisors are responsible for ensuring employees are trained on individual policies/procedure specific to their role.
2.1.12	HIPAA Research Policy	The HIPAA Research Policy must be reviewed prior to conducting: ▪ UAMS research activities that use or seek to use PHI about human subjects ▪ Research on PHI of deceased patients ▪ Review of PHI in preparation for research ▪ Limited Data Sets and Data Use Agreements
2.1.42	HIPAA Sanctions Policy	• Outlines procedures for disciplining UAMS employees for violations of HIPAA and UAMS HIPAA policies and procedures.
2.1.30	Information Access for Transfers and Terminations Additional resources: UAMS Administrative Guide 11.1.04 *Key Requests*	UAMS IT Security will implement procedures to ensure that UAMS Workforce members are granted appropriate access to ePHI. ePHI access will be terminated when the UAMS workforce member's employment ends or when a determination is made that such access should be terminated or otherwise modified. ▪ Departments are responsible for updating employee status in SAP on a timely basis. ▪ When the employment of a UAMS workforce member ends, their information systems privileges, both internal and remote, will be disabled. If the employee is dismissed

		involuntarily, it is the supervisor's responsibility to ensure compliance with these actions. ▪ Department supervisors are responsible for reviewing transferring employees' computer access levels and notifying the Department's IT Administrator or the UAMS IT Security Office of any computer system access levels that must be maintained, assigned or deactivated. ▪ Physical access to UAMS facilities after termination or transfer. Refer to 11.1.04 Key *Requests.*
2.1.35	Information Access Management	▪ Access to Confidential Information, including ePHI, is authorized on a "need-to know" basis ▪ UAMS has a formal documented process of determining who is granted access to the Confidential Information, including ePHI, and who grants this access. ▪ Formally designated UAMS Information Systems owners or their designees must define and authorize access to UAMS Information Systems containing Confidential Information approved by IT Security. ▪ UAMS Workforce members must not attempt to gain access to UAMS Information Systems for which they have not been given proper authorization. ▪ Revisions to access rights should be tracked and logged.
2.1.37	Information Security and Password Management	▪ Computers resources and software belong to UAMS and must be used in accordance with UAMS policy. Each campus department shall determine individual computer use. ▪ The use and/or copying of software shall be governed by license agreement. Illegal copying or distribution of software is strictly prohibited. ▪ All UAMS computers must have approved virus protection software installed and operational. ▪ UAMS maintains a formal, documented process for appropriately creating, changing, reviewing and safeguarding passwords used to validate a user's identity and establish access to its information systems and data. ▪ Unique passwords are required and must be a minimum of 8 characters and should be a combination of alphabetic, special and numeric characters. Password phrases or sentences of 12 characters or more are highly recommended for the UAMS domain log-in. Passwords should be changed periodically. Passwords should not be based on something that can be easily guessed or obtained using personal information. (e.g. names, favorite sports team, etc.) o Passwords must be kept confidential and not shared with anyone. o Avoid maintaining a paper record of passwords. o Change passwords whenever there is any indication of possible compromise. o Do not use the same password for personal and business accounts. o Change passwords at regular intervals and limit the re-using of old passwords on domain log-in accounts. o Change temporary password at the first log-on. ▪ Do not include passwords in any automated log-on process.
2.1.36	IT Risk Analysis and Risk Management of Electronic Systems	▪ UAMS conducts accurate and thorough assessments of the potential Risks and Vulnerabilities to the confidentiality, integrity, and Availability of Confidential Information, including Protected Health Information (PHI) and ePHI. ▪ UAMS takes effective steps to minimize or eliminate any such potential Risks and Vulnerabilities and continually assesses potential Risks and Vulnerabilities by developing, implementing, and maintaining appropriate Security Measures sufficient to reduce Risks and Vulnerabilities to a reasonable and appropriate level.
2.1.32	IT Security Incident Identification and Handling	▪ The IT Technical Security Team performs scans of the UAMS network to test for and identify any potential vulnerability present on workstations, servers, and other networked devices. ▪ All IT Security Incidents must be immediately reported to 686-8555.
2.1.24	Job Shadowing Policy	▪ The Department, Faculty Member or Staff who sponsors the Observer agrees to ensure that they comply with all UAMS policies. ▪ Applicants must be at least 16 years old and if under 18 must have written permission from a parent or legal guardian. ▪ Applicants must give at least one week notice prior to job shadowing and complete a Request to Shadow Form. ▪ If approved, the Applicant must have appropriate HIPAA training and sign a Confidentiality Statement and Hold Harmless Agreement (if under 18 a parent or legal guardian must sign). ▪ The Observer must be accompanied by a UAMS employee at all times and wear a name badge. ▪ Proper use and disclosure of PHI is the responsibility of the Department, Faculty Member or Staff and should be minimized. 1. Student Shadowers are prohibited from observing in the following areas: mental health, sexual assault, communicable disease, emergency department, and children under the age of eighteen (18) unless parent permission is obtained. 2. The job shadowing must not exceed one twelve-hour (12) shift.

2.1.10	Minimum Necessary	UAMS makes reasonable efforts to limit the use and disclosure of PHI to the minimum necessary to accomplish the purpose of the use or disclosure. This is not intended in any way to impede access to information necessary to provide treatment to our patients. **Some exclusions to the minimum necessary requirements include:** 1. Disclosure of a patient's PHI to a health care provider (outside UAMS) for treatment of that patient 2. Disclosures to the patient of his or her PHI 3. Use or Disclosure of PHI that is required by law or to comply with applicable laws and regulations ▪ UAMS physicians, nurses and other health care professionals will use professional judgment to determine the portions of the medical record needed for the purposes of **treatment** and may have access to the entire record if necessary for treatment purposes. ▪ All other uses and disclosures will be reviewed by persons having an understanding of our privacy policies and the expertise to understand and weigh the minimum necessary factors. 1. Except for the above exclusions, UAMS will only use, disclose, or request the entire medical record when it is specifically justified as being reasonably necessary to accomplish the intended purpose. 2. Authorized levels of access shall be determined by job classifications or functions. 3. UAMS personnel may reasonably rely on requests by: - Public health and law enforcement agencies or covered entities in determining the minimum necessary information - A professional who is a member of the UAMS workforce or is a business associate of UAMS if the professional represents that the information requested is the minimum necessary for the stated purpose - A researcher with appropriate documentation from an IRB or Privacy Board. Employees will only access PHI on a need-to-know basis for carrying out their specific job duties.
2.1.07	Mitigation of Uses/Disclosures in Violation of HIPAA	▪ UAMS will attempt to mitigate (lessen the harmful effects of) uses and disclosures that violate the HIPAA Regulations. ▪ Suspected improper uses and disclosures will be reported to the UAMS HIPAA Officer to coordinate the investigation and undertake mitigation efforts. ▪ If PHI is improperly used or disclosed by a Business Associate, appropriate action will be taken.
2.1.02	Mobile Device Safeguards	▪ Mobile devices containing Confidential Information must be encrypted when possible. ▪ Users are required to use the device's password protection feature and automatic time-out or password protected screen saver feature if available. ▪ Mobile Devices sent for outside repairs must have Confidential Information and PHI deleted and erased from storage or if Confidential Information and PHI is necessary for the repairs to be made a Business Associate Agreement must be in place with the vendor making the repairs. ▪ Security measures required by UAMS must be taken when sending Confidential Information or PHI in electronic form. ▪ Mobile Devices must be stored in a secure manner. ▪ Lost or stolen Mobile Devices containing Confidential Information or PHI must be reported to UAMS IT Security Officer (686-8555) and the UAMS Campus Police (686-7777) immediately. ▪ The Mobile Device user is responsible for deleting Confidential Information or PHI in a timely manner when storage in the device is no longer necessary. Upon termination of the user's employment or other relationship with UAMS, users must remove all Confidential Information from the Mobile Device.
2.1.06	Notice of Privacy Practices Additional Resources: Epic workflow for providing the NPP http://hipaa.uams.edu/content/Old/Compliance%20Slides%20Revised%2009262013.pdf .	UAMS patients are provided a Notice of Privacy Practices that describes how UAMS uses and discloses PHI, the patient's rights, and our legal duties. ▪ Patients with whom we have a direct treatment relationship are provided the Notice on first service date. ▪ A good faith effort is made to obtain the patient's written Acknowledgment of receipt of the Notice. If Acknowledgment is not obtained the reason is documented. ▪ In emergency situations, the provision of the Notice and its written Acknowledgment may be given as soon as reasonably practicable after the emergency treatment situation. ▪ The detailed workflow for providing the Notice at UAMS Medical Center is available at http://hipaa.uams.edu/content/Old/Compliance%20Slides%20Revised%2009262013.pdf.
2.1.19	Patient Information Restriction Requests	▪ Patients have the right to request restrictions on the use and disclosure of their PHI. ▪ UAMS is not required to agree to these requests. ▪ Requests must be submitted in writing on the Restriction Request Form. ▪ Requests must be routed to the UAMS HIPAA Office.

2.1.26	Patient Photography, Audio Recordings, Videography, and Other Imaging	Patient consent must be obtained prior to photography: ▪ For Treatment, Payment, or Healthcare Operations – Written Consent Required ▪ For All Other Purposes – Written Consent with valid HIPAA Authorization for ROI required ▪ Exceptions—Photographs taken for Identification Purposes, Documentation of Abuse & Neglect, De-identified Images, Family/Personal Use, and General recording or filming of premises for security purposes. ▪ Cessation of filing—patient has the right to request that filming or recording be stopped. Documentation: ▪ Should be date/time stamped and documented in patient's heath record if part of the treatment process. Devices: ▪ Security and Storage—Stored in a secure manner that protects the patient's privacy and defined by UAMS Policy. If applicable, a departmental policy should be in place. Photographs may not be stored on cameras. ▪ Patient copies-The patient is entitled to copies of photographs that are part of the patient's medical record. ▪ Research-Photography taken as part of a research protocol must be approved by the Institutional Review Board. ▪ Presentation/Publications—Written authorization must be obtained from the patient prior to using photographs. ▪ Non-UAMS Photographers taking photographs for UAMS—Must have a UAMS Confidentiality Agreement.
2.1.17	Patient's Request to Amend Medical Records or PHI	▪ Patients have the right to request an amendment of or correction to their medical record. ▪ UAMS is not required to agree to these requests. ▪ Routine requests to change a patient's contact information or other non-medical information are not required to be in writing and are handled according to the appropriate departmental policy. ▪ All other requests should be submitted to the HIM department for processing using the "Request for Amendment of Health Information Form."
2.1.28	Protected Health Information Breach Notification and Reporting	▪ All possible breaches of PHI must be reported to the UAMS HIPAA Office immediately by calling 501-603-1379 or e-mailing HIPAA@uams.edu. ▪ All lost equipment (computers, laptops, smartphones, alphanumeric pages, thumb drives, CD's or DVD's) possibly containing PHI must be reported immediately to UAMS IT Security by calling the IT Helpdesk at 686-8555. ▪ All thefts and suspected thefts involving PHI must also be reported to law enforcement immediately. ▪ All documents possibly involved in a breach should be retained and turned over to the UAMS HIPAA Office. ▪ The UAMS HIPAA Office will coordinate and manage all patient notifications. ▪ The UAMS HIPAA Office will review all breaches and maintain breach reporting records.
2.1.09	Psychotherapy Notes	See definition of Psychotherapy Notes. Use and disclosure of Psychotherapy Notes without prior patient authorization is very limited and includes: ▪ Use by the originator of the notes for treatment. ▪ Use or disclosure by UAMS for its own mental health training programs. Employees who create or maintain PHI that meets the definition of Psychotherapy Notes should review this policy in detail.
2.1.05	Release of Patient Directory Information Additional resource: Confidential and Private Encounter Patients, Putting it All Together Epic Tip Sheet http://intranet.uams.edu/cctc/Training/Info/UConnect_Training/Tip-Sheets/Cadence_Patient%20Types--%20Confidential%20(Break%20the%20Glass)%20and%20Private%20Encounter.pdf UAMS Nursing Manual	▪ Unless the patient requests UAMS not to disclose Patient Directory Information, UAMS may provide Patient Directory Information to a person, provided that the requesting party specifies the patient's name. ▪ The following is considered UAMS Patient Directory information: 1. Patient name 2. Location in our facility 3. One word statement of condition 4. Religious affiliation – only released to the clergy ▪ Patients may restrict or prohibit release of directory information. UAMS will "flag" as "no info". In Epic, patients who have opted out of the Directory are registered as Private Encounter: Yes. ▪ UAMS also may elect on its own, without a patient's request, to exclude patients from the directory and not release information. An example would be for safety reasons. ▪ Members of the media who request information will be referred to the Office of Communications and Marketing at 686-8990. ▪ Requests for condition will be referred to the nursing unit except for requests from members of the media. ▪ For detailed work flow refer to Epic Tip Sheet

		▪ For a list of one word statements of condition refer to the UAMS Clinical Programs Nursing Manual.
2.1.08	Reporting of HIPAA Violations	▪ All known or suspected violations of these policies or the HIPAA regulations must be reported. ▪ There will be no retaliation for reporting in good faith. ▪ Reports can be made to: 1. Reporting line at 1-888-729-2755 or 501-614-2187 2. UAMS HIPAA Office 501-603-1379 or HIPAA@uams.edu 3. Go to http://hipaa.uams.edu and click on Report an Incident tab 4. UAMS Research Compliance Office 501-686-5667 5. UAMS IT Security Office 501-603-1336 5. Anyone in a position of responsibility. The person receiving the report must then contact the HIPAA Office.
2.1.03	Request for Alternative Method of Communications of PHI Additional resources: *UAMS Medical Center Request for Alternative Method of Communications PS.2.10* *Temporary Address Epic Tip sheet* http://intranet.uams.edu/cctc/Training/Info/UConnect_Training/Tip-Sheets/Cadence_ADT_Temporary_Address.pdf	▪ Patients may request UAMS utilize alternative methods (e.g., written/verbal) or alternative locations (e.g., work/home) to communicate with them. ▪ Reasonable requests will be honored. ▪ UAMS Medical Center will utilize the temporary address fields in Epic to operationalize these requests. ▪ If information is in the temporary fields, it must be utilized to communicate with patients. ▪ When Alternate Methods of Communication requests are received, refer to UAMS Medical Center Policy PS.2.10.
2.1.14	Requests for Data Extracts	• IT maintains an inventory of databases containing PHI. All databases must be reported to IT. • Requests for data extracts must contain information specified in the policy. A sample request form is included. • The date the extract was performed and the request form must be kept for a minimum of six years. • The UAMS HIPAA Office must approve requests for data extracts to be disclosed outside UAMS, including requests by individuals who are not members of the UAMS workforce.
2.1.23	Safeguarding of PHI	This policy contains procedures to “safeguard” PHI from use or disclosure in violation of the HIPAA regulations and addresses: ▪ Protecting Printed Information ▪ Bulletin Boards ▪ Storage of Paper-Based Data ▪ Shredders and Outsourcing Shredding ▪ Destruction of Electronic Storage Media/Devices ▪ Physical Security ▪ Logical Security such as user authentication and passwords ▪ Conversations ▪ Overhead paging ▪ X-Ray Lightboards, Whiteboards and Patient Tracker Boards ▪ Sign-in Sheets ▪ Charts in Chart Holders Outside Exam Rooms ▪ Voice Mail/Answering Machine Messages ▪ Email ▪ Vocera Communication ▪ Social Networking ▪ Faxing ▪ Safeguarding ePHI and Other Confidential Information in Electronic Format ▪ Transporting and/or Accessing UAMS Confidential Information off campus.
2.1.20	Use and Disclosure of PHI for Fundraising	HIPAA imposes strict rules regarding the use or disclosure of PHI for fundraising purposes, and HIPAA permits PHI to be used or disclosed only under limited circumstances. Information which would disclose the nature of the services received by a patient (even if limited to just the department of service, such as otolaryngology, cardiology, psychiatry), or the identity of the physician associated with that patient, cannot be used or disclosed for fundraising purposes without the patient’s authorization. ▪ See the UAMS Authorization for Fundraising Form. - All fundraising materials sent to a patient must include instructions on how to opt out of receiving future fundraising communications. - Consult the UAMS HIPAA Office if you have questions.

2.1.13	Use and Disclosures of PHI and Medical Records	This policy is the main policy regarding the way in which UAMS uses and discloses patient information. ▪ General Information – Signed authorizations, verification of identity/authority ▪ Disclosures to the Patient ▪ Disclosures for UAMS Treatment, Payment and Operations (TPO) – note PHI may be used or disclosed for our own TPO without patient authorization subject to the minimum necessary requirements and any patient restrictions we have agreed to ▪ Disclosures to another health care provider or covered entity. ▪ Patient Request for Access to or a Copy of Medical Records. ▪ Disclosures to Patient's Legal Representative (includes list of who constitutes a legal representative.) ▪ Disclosures to Spouse/family/friends Involved in the Patient's Care. ▪ Patient Authorization Form - includes required elements of a valid authorization ▪ Disclosure of Information Outside UAMS for Purposes Unrelated to Treatment, Payment and Operations ▪ Disclosures Required by Law ▪ Reporting to Agencies or Others Authorized by Law to Receive the Information ▪ Court Orders, Warrants, and Grand Jury Subpoenas ▪ Subpoenas and Discovery Requests from Parties in Litigation ▪ Subpoenas from Law Enforcement Officials ▪ Law Enforcement Generally (Without Court Order, Warrant, Subpoena) ▪ Adult Victims of Abuse, Neglect or Domestic Violence ▪ Adult Victims of Rape, Attempted Rape, Sexual Assault or Incest ▪ Substance Abuse/Treatment Information ▪ Minors ▪ Patient Request to Amend Record ▪ Cost of Obtaining Copies of Medical Records ▪ Sanctions/Disciplinary Action Attachment – Copies of UAMS Authorizations for Release of Information
2.1.21	Use of PHI for Marketing	UAMS will not use or disclose PHI for marketing purposes without a signed HIPAA Authorization from the patient, except as allowed by federal and state law, including the Federal HIPAA Privacy Regulations. Marketing means communications about a product or service that encourages recipients of the communication to purchase or use the product or service. For the purpose of this policy, Marketing <u>does not include</u>: 1. Communications to the patient for the purpose of describing a health-related product or service that is provided by UAMS, or included in a UAMS plan of benefits. 2. Communications to the patient that are a part of treatment of the patient. 3. Communications to the patient in the course of coordinating treatment or for the purpose of recommending alternative treatments, therapies, health care providers or setting of care. Except as allowed by this policy, UAMS will obtain the patient's authorization in writing prior to using or disclosing a patient's PHI for marketing purposes. UAMS is not required to obtain authorization for marketing communications under the following circumstances: 1. Face to face communication between UAMS and the patient; or 2. UAMS provides the patient a promotional gift of nominal value, i.e. items with our name or another company's name, or sample products. ▪ If UAMS engages a third party for the purpose of communication with individuals about a product or services of UAMS, a business associate agreement is required. This situation requires prior patient Authorization.
2.1.22	Verification of Identity and Authority to Receive PHI	▪ If the identity or authority of a person requesting PHI is not known to you, their identity and authority to have the PHI must be verified prior to providing any PHI. ▪ Follow procedures developed in your specific area to verify identity and authority of requestors of PHI. Examples are included in the policy. ▪ A valid driver's license can be used to verify identity. ▪ The identity of public officials can be verified by: - Agency ID badge or other official credentials - A written request on appropriate letterhead - Written statement that requestor is acting on behalf of a public official ▪ Authority to act as a patient's legal representative for healthcare matters must be established before release of PHI. "Legal Representative" does not mean a patient's attorney. ▪ **Exceptions to the verification of identity include:** - Not required for Patient Directory disclosures - Not required when patient has signed authorization to mail PHI to address specified on authorization.