



Faculty Resources
Teaching Healing Searching Serving

[Faculty Resources Home](#)

[UAMS Home](#)

[Academic Affairs Home](#)

[Colleges](#)

- College of Medicine
- College of Nursing
- College of Pharmacy
- College of Health
Related Professions
- College of Public Health
- Graduate School

[Helpful Links](#)

[FAQs](#)

[Campus Directory](#)

[Intranet](#)

[Contact Us](#)

Faculty Resources

7. UAMS HIPAA Policies and Services

[Accounting for Disclosure](#) (Admin Guide 3.1.26)

[Business Associate Policy](#) (Admin Guide 3.1.33)

[Confidentiality Policy](#) (Admin Guide 3.1.15)

[Creating Revision of UAMS Policies Involving HIPAA Administrative, Security or Privacy Requirements](#) (Admin Guide 3.1.39)

[De Identification of Protected Health Information and Limited Data Set Information](#) (Admin Guide 3.1.31)

[HIPAA Education and Training](#) (Admin Guide 3.1.30)

[HIPAA Research Policy](#) (Admin Guide 3.1.27)

[Information Access or Transfers and Terminations](#) (Admin Guide 3.1.41)

[Minimum Necessary Policy](#) (Admin Guide 3.1.25)

[Mitigation of Uses/Disclosures in Violation of HIPAA](#) (Admin Guide 3.1.22)

[Mobile Device Safeguards](#) (Admin Guide 3.1.17)

[Notice of Privacy Practices](#) (Admin Guide 3.1.21)

[Patient Information Restriction Requests](#) (Admin Guide 3.1.34)

[Patient Request to Amend Medical Records or PHI](#) (Admin Guide 3.1.32)

[Policy on Use of PHI for Fundraising](#) (Admin Guide 3.1.35)

[Psychotherapy Notes Policy](#) (Admin Guide 3.1.24)

[Request for Alternative Method of Communications of Protected Health Information](#) (Admin Guide 3.1.18)

[Releasing of Patient Directory Information](#) (Admin Guide 3.1.20)

[Reporting of HIPAA Violations](#) (Admin Guide 3.1.23)

[Request for Extracts](#) (Admin Guide 3.1.29)

[Safeguarding Protected Health Information](#) (Admin Guide 3.1.38)

[Use and Disclosure of PHI and Medical Records](#) (Admin Guide 3.1.28)

[Use of PHI for Marketing](#) (Admin Guide 3.1.36)

[Verification of Identity](#) (Admin Guide 3.1.37)

[Working from Home](#) (Admin Guide 3.1.40)

Assistance and more information is available through the UAMS [HIPAA Office](#) (<http://hipaa.uams.edu/>).



[Back](#)

10/13/2005



UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.26

DATE: 04/01/03

REVISION: 03/01/04

SECTION: ADMINISTRATION
AREA: GENERAL ADMINISTRATION
SUBJECT: ACCOUNTING FOR DISCLOSURES

SCOPE

UAMS Workforce

DEFINITIONS

Accounting for Disclosures is a method of documenting and tracking certain types of disclosures of Protected Health Information (PHI) made by UAMS, verbally or in writing, to persons or entities who are not a part of UAMS.

Disclosure means the release, transfer, provision of access to, or divulging of information in any manner (verbally or in writing) by UAMS to persons who are not UAMS employees or students, or to any other person or entity **OUTSIDE** of UAMS.

Protected Health Information (PHI) means information that is part of an individual's health information that identifies the individual or there is a reasonable basis to believe the information could be used to identify the individual, including demographic information, and that (i) relates to the past, present or future physical or mental health or condition of the individual; (ii) relates to the provision of health care services to the individual; or (iii) relates to the past, present, or future payment for the provision of health care services to an individual. This includes PHI which is recorded or transmitted in any form or medium (verbally, or in writing, or electronically). PHI excludes health information maintained in educational records covered by the federal Family Educational Rights Privacy Act and health information about UAMS employees maintained by UAMS in its role as an employer.

UAMS Workforce means physicians, employees, volunteers, residents, students, trainees, visiting faculty, and other persons whose conduct, in the performance of work for UAMS, is under the direct control of UAMS, whether or not they are paid by UAMS.

POLICY

UAMS will establish and maintain a system for Accounting of Disclosures as required by HIPAA.

Beginning April 14, 2003, a UAMS patient may request an Accounting of Disclosures of his or her own PHI for up to a period of six years prior to the patient's date of request. UAMS is not required to account for any disclosures made prior to April 14, 2003

- A. **Disclosures Exempt From Accounting:** The following types of disclosures do **NOT** have to be included in the Accounting of Disclosures. Disclosures that were made:
1. for treatment of the patient, for payment of or reimbursement for healthcare services provided to the

patient, or for health care operations see UAMS [Use and Disclosure of PHI and Medical Records Policy, 3.1.28](#) for more information on the use and disclosure of PHI for treatment, payment and health care operations which do not require patient authorizations or accounting for disclosures;

2. directly to the patient about their own information;
3. disclosures permitted by a signed patient authorization;
4. from a patient directory;
5. to individuals involved in the patient's care;
6. for national security or other intelligence purposes;
7. incident to a permitted use or disclosure;
8. for purposes of a Limited Data Set in which the patient's information that could identify the patient is excluded from the Data Set;
9. to correctional institutions or law enforcement when the patient is an inmate or otherwise in their lawful custody;
10. disclosures to and by Business Associates with whom UAMS has a Business Associate agreement, as long as the disclosures are for an exempt purpose, such as for payment or health care operations of UAMS; or
11. any disclosures made prior to April 14, 2003.

B. Disclosures Subject to Accounting Requirement: Except for any disclosures described above in Paragraph I, disclosures required or allowed by law without patient authorization must be included in the accounting. (Also refer to applicable section of the UAMS Use and [Disclosure of PHI and Medical Records Policy, #3.1.28](#)).

Examples of disclosures which **MUST BE INCLUDED** in an accounting include, but are not limited to, the following disclosures (if there is no signed authorization by the patient that meets the HIPAA authorization requirements set forth in the UAMS [Use and Disclosure of PHI and Medical Records Policy, #3.1.28](#)).

1. Arkansas Department of Health for TB, HIV, STD, or other infectious disease reporting.
2. Arkansas Department of Health for State Health Data Clearinghouse reporting;
3. Arkansas Department of Health, Division of Vital Records, for reporting of births or deaths;
4. FDA reporting for death, adverse event, or devices subject to tracking;
5. Organ, eye and tissue donation agencies;
6. Registries outside of UAMS which require disclosures, such as Cancer Registry, Immunization Registry, and Trauma Registry;
7. Spinal Cord injury reporting;
8. Cases of abuse/neglect requiring reporting to authorities;
9. County Coroner or County Sheriff for sudden infant death cases;

10. County Sheriff and City Policy to report intentional infliction of knife or gunshot wounds;
 11. U.S. Department of Health and Human Services for purposes of investigating or determining UAMS' compliance with HIPAA regulations;
 12. Coroners and Medical Examiners to identify a deceased person or to determine cause of death or to perform other duties authorized by law;
 13. State Crime Lab, if (1) specimen is accompanied by a label with PHI on it; and (2) release is performed without authorization;
 14. Funeral Directors;
 15. Courts or administrative agencies in response to subpoena, warrant, or similar process authorized by law;
 16. Other law enforcement purposes, such as providing PHI to law enforcement about a suspected or actual crime victim, and to avert a serious threat to the health or safety of a person or to the public (unless law enforcement has requested that accounting not be provided for a specified period of time);
 17. Disclosures to and by Business Associates with whom UAMS has a Business Associate agreement, **only if** the disclosures are not for an exempt purpose, such as for payment or health care operations of UAMS.
- C. Research:** UAMS must provide an accounting of disclosures of PHI in connection with research projects when there is no patient authorization for the disclosures, unless the disclosures are limited to PHI furnished in Limited Data Sets to recipients under a Data Use Agreement or a De-identified Record Set as defined in the UAMS [De-Identification of PHI Policy, #3.1.31](#). UAMS must provide an accounting of disclosures of PHI pursuant to the waiver process. Refer to UAMS [HIPAA Research Policy, #3.1.27](#) for more information regarding the accounting of disclosure requirements for Research.
- D. For Victims of Neglect, Domestic, or Child Abuse:** UAMS must provide an accounting of disclosures made for these purposes unless specifically exempted. In cases of domestic or child abuse, if UAMS has reason to believe that release to the patient's personal representative could endanger the patient, UAMS has the discretion to decline the request.
- E. Temporary Suspension of Request for Accounting:** UAMS may temporarily suspend granting a patient's request for an accounting if a health oversight agency or law enforcement official has provided UAMS with a written statement that the accounting to the patient may likely impede their activities. The written statement must also specify the time for the suspension. If the statement from the agency or official is made orally, then the suspension is limited to no longer than 30 days. UAMS must document the statement and the identity of the agency or official making the statement.
- F. Time Period for Complying with Request for Accounting:** UAMS must provide the patient with the accounting within **sixty (60) days** of the request. If unable to do so, UAMS must provide the patient with a written explanation for the delay and the date by which the accounting will be provided, not to exceed 90 days from the date of the request. This extension is permitted only once on a request for accounting.
- G. Fees/Charges:** The first accounting requested by the patient in any 12-month period is free. For each subsequent request by the patient *in the same* 12-month period, UAMS may charge a reasonable, cost-based fee, including reasonable retrieval and report preparation costs, as well as any mailing costs, only if the patient knows of such fees in advance and has the opportunity to withdraw or modify the request to avoid or reduce the fee.

PROCEDURE

A. Recording Data for Accounting:

1. UAMS will maintain the information necessary to provide an Accounting. Employees provided access to the “UAMS Release and Disclosure System” software or those employees utilizing a manual or other electronic disclosure

Accounting system must record all required information for **each** disclosure that is subject to accounting.

2. All data must be recorded on the “UAMS Release and Disclosure System” by direct electronic entry or manual or other electronic entry on a copy of the Disclosure Reporting form (attached) or by manual entry on an Accounting Log Form (attached) or other Accounting form kept in the patient’s medical record or other official file. The information recorded must include:
 - a. The date of disclosure;
 - b. The name/address of entity or person receiving the PHI;
 - c. A brief description of the PHI disclosed; and
 - d. Either a brief statement of the purpose of the disclosure that reasonably informs the patient of the basis of the disclosure; a copy of the patient’s written authorization for the disclosure, or a copy of the written request for the disclosure, if any.
3. For multiple disclosures the accounting may provide the information in Item 2 above for the first disclosure, the frequency or number of disclosures made during such period and date of the last disclosure during the period.

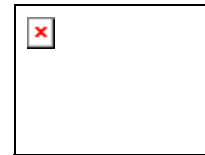
B. Obtaining and Accounting of Disclosure:

1. Patients or authorized individuals will be directed to the Medical Records Department to request the Accounting. Requests for Accountings must be made in writing by using the attached Accounting of Disclosures form.
2. The Medical Records Department will process the request and give or mail the Accounting to the patient or authorized individual. Records personnel must record the date of the request and the date and name of the individual receiving the accounting.

Please use Word file forms (click on document icon at the top of page)

Patient Label if Available **OR**

Print Patient Name



Request for an Accounting of Disclosures

Date of Request: _____

Patient Name: _____

Date of Birth : _____

Medical Record Number: _____

Patient Address :

Address to send accounting of disclosure (if different than above):

Dates Requested:

I would like an accounting of disclosures for the following time frame:

(Please note: The earliest "from date" is April 14, 2003.)

From: ____/____/____ To: ____/____/____

(no earlier than April 14, 2003)

Fees:

The first request in a 12-month period is free.

There may be a charge for subsequent requests in that same 12-month period

The fee for this request will be: _____

I understand that there may be a fee for this accounting, and I wish to proceed with my request. I also understand that the accounting will be provided to me within 60 days unless I am notified in writing that an extension of up to 30 days is needed.

_____ Signature of Patient or Legal Representative

Date

If Legal Representative, authority of Legal Representative _____

(such as parent of a minor, court-appointed guardian, administrator of estate of deceased, attorney-in-fact appointed with power of attorney, or healthcare proxy)

For Healthcare Organization Use Only:

Date Received: _____ Date Accounting Sent: _____

Extension Requested: No Yes Reason: _____

Patient notified in writing on this date: _____

Staff Member Processing Request: _____

Place Patient Label Here **or**

UNIVERSITY OF ARKANSAS
FOR MEDICAL SCIENCES

Disclosure Reporting Form

Instructions: This form is used to document patient disclosures that are subject to a patient's request for an "Accounting of Disclosures." Refer to Accounting of Disclosures Policy. Fill out the information below and send the form to Slot 524.

Name of the person making the disclosure: _____

Location: _____

Phone #: _____

* * * * *

Patient Name: _____

Last Name / First Name / MI

Date of birth: _____

Medical Record #: _____

Brief description of the information disclosed.

Date of the disclosure: _____ (MM/DD/YYYY)

Brief statement of the purpose of the disclosure.

Name of person or entity who received the information and address (if known).

Name of person filling out this form, if different than above:



UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.33

DATE: 04/01/03

REVISION: 03/01/04

SECTION: ADMINISTRATION
AREA: GENERAL ADMINISTRATION
SUBJECT: BUSINESS ASSOCIATE POLICY

COPE

JAMS Workforce

DEFINITIONS

Business Associate is a person or entity who is not a member of the UAMS Workforce, and who performs or assists in the performance of, a function of activity *for or on behalf of UAMS* which involves disclosures that are regulated and permitted by HIPAA and which involve the creation, use or disclosure of Protected Health Information by the Business Associate.

Designated Record Set means a group of records maintained by or for UAMS in which the records are (i) medical records and billing records about patients maintained by or for UAMS; or (ii) enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) records used, in whole or in part, by or for UAMS to make decisions about patients. For purposes of the term “records” in this definition of Designated Record Set, this includes any item, collection or grouping of information that includes Protected Health Information and is maintained, collected, used or disseminated by or for UAMS.

Disclosure means the release, transfer, providing access to, or divulging of Protected Health Information in any other manner (verbally or in writing) outside of UAMS.

Healthcare Operations is defined by the HIPAA regulations under 45 C.F.R. § 164.501 and is incorporated herein by reference, and includes, but is not limited to, the following:

- a. Quality assessment and improvement, including outcomes evaluation and development of clinical guidelines; population-based activities relating to improving health, protocol development, case management and case coordination, contacting providers and patients with information about treatment alternatives; and related functions that do not include treatment.
- b. Accreditation, certification, licensing or credentialing activities, reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals.
- c. Conducting or arranging for medical review, legal services and auditing.
- d. Business planning and development related to managing and operating the entity.
- e. Business management and general administrative activities, such as fundraising and marketing of services to the extent permitted without authorization, disclosure of PHI in a due diligence review or to resolve internal grievances, and customer service.

Organized Health Care Arrangement (“OHCA”) means (i) a clinically integrated care setting in which individuals typically receive health care from more than one health care provider; or (ii) an organized system of

health care in which more than one covered entity participates, and in which the participating covered entities hold themselves out to the public as participating in a joint arrangement and participate in joint activities of at least one of the following: utilization review, quality assessment/improvement activities, or payment activities if the financial risk for delivering health care is shared, in whole or in part, by the participating covered entities. See HIPAA regulations for a more complete definition.

Payment includes billing, reimbursement, and collection activities relating to the provision of healthcare to an individual, including but not limited to, release to an insurance company, insurance plan or other third-party payer in connection with payment activities, eligibility or coverage determinations, disclosures to consumer reporting agencies, healthcare data processing, claims management and other activities as defined by 45 C.F.R. § 164.501 under “payment.”

Protected Health Information (PHI) means information that is part of an individual’s health information that identifies the individual or there is a reasonable basis to believe the information could be used to identify the individual, including demographic information, and that (i) relates to the past, present or future physical or mental health or condition of the individual; (ii) relates to the provision of health care services to the individual; or (iii) relates to the past, present, or future payment for the provision of health care services to an individual. This includes PHI which is recorded or transmitted in any form or medium (verbally, or in writing, or electronically). PHI excludes health information maintained in educational records covered by the federal Family Educational Rights Privacy Act and health information about UAMS employees maintained by UAMS in its role as an employer.

Required by Law: “Required by Law” generally means a requirement in the law that compels a person or entity to act or prohibits a person or entity from acting and that is enforceable in a court of law, including the requirements of any applicable federal or state laws and regulations.

UAMS Workforce: UAMS Workforce includes UAMS physicians, employees, volunteers, residents, students, trainees, visiting faculty, and other persons whose conduct, in the performance of work for UAMS, is under the direct control of UAMS, whether or not they are paid by UAMS.

POLICY

Prior to disclosing any Protected Health Information to a Business Associate of UAMS, UAMS will obtain satisfactory assurances from a Business Associate that the Business Associate will appropriately safeguard the Protected Health information it receives or creates on behalf of UAMS. UAMS will document these satisfactory assurances in writing in the form of a Business Associate Agreement or other written agreement with the Business Associate in compliance with the HIPAA regulations. Any disclosures to a Business Associate must be limited to disclosures permitted by the HIPAA regulations and not for the Business Associate’s independent use or purposes.

PROCEDURES

i. DETERMINE IF PERSON or ENTITY IS A BUSINESS ASSOCIATE.

Based on the definition of “Business Associate” as stated in this Policy, a Business Associate is not a member of the UAMS Workforce. A Business Associate generally is a person or entity that performs certain functions or activities on behalf of UAMS, or provides services to UAMS, that are regulated and permitted by HIPAA, such as disclosures for purposes of Payment or Healthcare Operations *and* which involve the creation, use or disclosure of PHI.

Examples of a Business Associate may include:

- A vendor who provides billing or collection services for UAMS.
- A consultant to review the accuracy of billing and coding practices.

- A company who provides document shredding services to UAMS for the purpose of shredding documents containing PHI.
- An attorney who assists in assessing UAMS' compliance with federal billing laws and regulations, who is hired in connection with allegations of malpractice, or who advises a hospital on medical staff disciplinary matters.
- A person who provides medical transcription services for UAMS.

B. NO BUSINESS ASSOCIATE RELATIONSHIP. The following situations are examples of situations where a Business Associate relationship is **not** created:

1. **Provider to Provider.** Disclosures of PHI between UAMS and a health care provider outside of UAMS for the purpose of patient treatment, including a physician or hospital laboratory disclosing PHI to an outside laboratory to diagnose an individual.
2. **Service or Maintenance Vendors Without Exposure to PHI.** Relationships with persons or organizations, such as janitorial services, electricians, or copier repair companies, whose functions or services are not intended to involve the use or disclosure of PHI, and where any disclosure of PHI during the performance of their duties would be limited and incidental, such as disclosures that may occur while walking through or working in file rooms. **NOTE:** If a service is hired to do work for UAMS where disclosure of PHI is not limited in nature (such as routine handling of records or shredding of documents containing protected health information), it likely would be a Business Associate.
3. **Couriers.** Disclosures of PHI by UAMS to a person or organization that acts merely as a conduit for protected health information, such as the U.S. Postal Service, UPS, Federal Express, other private couriers, and their electronic equivalents.
4. **OHCA.** Disclosures of PHI between UAMS and other covered entities with whom UAMS participates in an OHCA where the PHI relates to the joint health care activities of the OHCA.
5. **Financial Transaction Institutions.** When a financial institution processes consumer-conducted financial transactions by debit, credit, or other payment card, clears checks, initiates or processes electronic funds transfers, or conducts any other activity that directly facilitates or effects the transfer of funds for payment for health care or health plan premiums. When it conducts these activities, the financial institution is providing its normal banking or other financial transaction services to its customers; it is not performing a function or activity for, or on behalf of, UAMS.
6. **No PHI Disclosed.** If the information disclosed is not PHI, or if the PHI is de-identified in accordance with the UAMS [*De-Identification of Protected Health Information and Limited Data Set Information Policy 3.1.31*](#), then the person or entity receiving the information would not be a "Business Associate."

C. DISCLOSURES TO A BUSINESS ASSOCIATE: UAMS may not disclose PHI to a Business Associate or allow a Business Associate to create or receive PHI on behalf of UAMS until UAMS obtains satisfactory assurance that the Business Associate will appropriately safeguard the information as required by the HIPAA regulations. This satisfactory assurance must be documented in writing in the form of a contract, agreement or other written arrangement, and must also include the obligations of UAMS with regard to the PHI to be held by the Business Associate.

D. DISCLOSURES TO BUSINESS ASSOCIATE OF ANOTHER. UAMS may share PHI directly with the

Business Associate acting on behalf of another, as long as the disclosure is one that is permitted by HIPAA.

- E. DISCLOSE ONLY MINIMUM NECESSARY.** UAMS will disclose to a Business Associate only the PHI that is reasonably necessary to accomplish the intended purpose of the disclosure. See UAMS [Minimum Necessary Policy 3.1.25](#) for more information. Under a Business Associate Agreement, the Business Associate must request only the information that is the “minimum necessary”, and therefore, UAMS may reasonably rely on a request from a Business Associate, or the Business Associate or another, to be a request for PHI that meets the minimum necessary standards.
- F. DISCLOSURES THROUGH A LIMITED DATA SET – NO BUSINESS ASSOCIATE AGREEMENT REQUIRED.** When UAMS discloses information to a Business Associate through the use of a “Limited Data Set” (where most of the PHI is de-identified so that the patient’s identity cannot be determined) pursuant to the UAMS [De-Identification of Protected Health Information and Limited Data Set Information Policy 3.1.31](#), a Business Associate Agreement is not required. Only a Data Use Agreement is required.
- G. DISCLOSURES FOR PURPOSES OF RESEARCH.** See UAMS [Research Policy 3.1.27](#).
- H. DATA AGGREGATION SERVICES.** “Data Aggregation Service” means the combining of PHI of one covered entity, such as UAMS, with the PHI of another covered entity, such as another hospital. When the Data Aggregation Service is performed by the Business Associate of both covered entities to permit data analyses relating to the Healthcare Operations of the respective covered entities, this is a disclosure of PHI that is permitted by HIPAA. In the absence of the Business Associate arrangement involving Data Aggregation Services, the ability of the participating covered entities, such as two hospitals, to share the PHI with one another would be restricted under HIPAA.
- I. BUSINESS ASSOCIATE AGREEMENTS:** If the person or entity meets the definition of a “Business Associate,” a contract or other written arrangement is required to document the assurances from the Business Associate that the Business Associate will appropriately safeguard the Protected Health information it receives or creates on behalf of UAMS. This contract or other written arrangement will be referred to in this Policy as the “Business Associate Agreement.”
- 1. Agreement Must Establish Permitted/Required Uses and Disclosures.** The Business Associate Agreement between UAMS and a Business Associate must establish the permitted and required uses and disclosures of PHI by the Business Associate on behalf of UAMS.
 - 2. Agreement Must Prohibit Use and Further Disclosures in Violation of HIPAA.** UAMS will not authorize a Business Associate to use or further disclose PHI in a manner that would violate the HIPAA privacy Regulations if such use or disclosure were done by UAMS.
 - 3. Agreement Must Authorize Termination of Contract if Violations by Business Associates.** The Business Associate Agreement between UAMS and a Business Associate must authorize UAMS to terminate the contract if UAMS determines that the Business Associate has violated a material term of the contract.
 - 4. Other Required Provisions:** In its Business Associate Agreement contract with a Business Associate, UAMS must provide that the Business Associate will:
 - a. Not use or further disclose PHI other than as permitted or required by the contract or as required by law;
 - b. Use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by its contract;
 - c. Report to UAMS any use or disclosure of PHI not provided for by its contract of which the Business Associate becomes aware;

- d. Ensure that any agents, including a subcontractor, to whom it provides PHI received from, or created or received by the Business Associate on behalf of, UAMS agrees to the same restrictions and conditions that apply to the Business Associate with respect to such information;
- e. Make any PHI available to UAMS to allow UAMS to comply with HIPAA regulations requiring an individual with access to, or a copy of, the individual's PHI contained in a Designated Record Set;
- f. Make any PHI available to UAMS necessary for UAMS to amend the PHI and incorporate any amendments to the PHI in accordance with HIPAA regulations if UAMS has agreed to or required such amendment;
- g. Make available to UAMS the information required to provide an accounting of disclosures in accordance with the HIPAA regulations;
- h. Make its internal practices, books, and records, relating to the use and disclosure of Protected Health Information received from UAMS, or created or received by the Business Associate on behalf of UAMS, available to UAMS or to the Secretary of the United States Department of Health and Human Services; and
- i. Upon termination of its contract with UAMS, return or destroy all PHI received from UAMS, or created or received by Business Associate on behalf of UAMS, that the Business Associate still maintains in any form and retain no copies of such information; or, if such return or destruction is not feasible, the obligations of the Business Associate contained in the Business Associate Agreement shall extend beyond termination of the contract for so long as the Business Associate maintains such PHI.

5. Agreement May Permit Other Uses. The Business Associate Agreement may permit the Business Associate to use PHI received by the Business Associate in its capacity as a Business Associate to UAMS, only if such use is necessary for (a) the proper management and administration of the Business Associate; or (b) to carry out the legal responsibilities of the business associate.

6. Agreement May Permit Other Disclosures: The Business Associate Agreement may permit the Business Associate to disclose PHI received by the Business Associate in its capacity as a Business Associate to UAMS, ONLY if such disclosure is necessary for (a) the proper management and administration of the Business Associate; or (b) to carry out the legal responsibilities of the business associate; however, prior to either type of disclosure, the following must occur:

The Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

7. Agreement May Permit Data Aggregation Services. In its Business Associate Agreement with a Business Associate, UAMS may permit the Business Associate to provide Data Aggregation Services relating to the Healthcare Operations of UAMS.

J. NON-COMPLIANCE BY BUSINESS ASSOCIATE: If UAMS has actual knowledge of a pattern of activity or practice of the Business Associate that constitutes a material breach or violation of the an obligation of the Business Associate under the Business Associate Agreement or other written contract evidencing the Business Associate Agreement, UAMS must take reasonable steps to cure the breach or end the violation, as applicable, and if such steps are unsuccessful, UAMS must:

- 1. terminate the contract or arrangement with the Business Associate, if feasible; or if termination is not feasible, report the problem to the Secretary of the United States Department Health and Human

Services; and

2. mitigate, to the extent practicable, any harm effect that is known to UAMS arising from a disclosure of PHI in violation of the UAMS policies and procedures or the HIPAA regulations.

K. TRANSITION PERIOD FOR EXISTING CONTRACTS.

For the persons or entities who meet the definition of a Business Associate of UAMS and who had an existing contract or other agreement with UAMS prior to October 15, 2002, UAMS may continue to operate under that contract until April 14, 2004, or until the contract is renewed or modified, whichever is sooner. This includes contracts that renew automatically without any change in terms or other action by the parties and that exist by October 15, 2002. Renewal or modification requires action by the parties involved. For example, an automatic inflation adjustment to the price of a contract does not trigger the end of the transition period, nor make the contract ineligible for the transition period if the adjustment occurs before April 14, 2003.

This transition period applies only to written contracts or other written arrangements. Oral contracts or other arrangements are not eligible for the transition period.

During the transition period, UAMS may only disclose PHI to a Business Associate for a purpose permitted by the HIPAA Privacy Regulations, and UAMS must apply the minimum necessary standard, as appropriate, to such disclosures. However, UAMS is not required to obtain a Business Associate Agreement during this period.

During the transition period, UAMS must ensure, in whatever reasonable manner deemed effective by UAMS, the appropriate cooperation by its Business Associates in meeting the following requirements during the transition period:

- a. Make information available to the Secretary, including information held by a business associate, as necessary for the Secretary to determine compliance by the covered entity.
- b. Fulfill a patient's rights to access and amend his or her PHI contained in a Designated Record Set, including information held by a Business Associate, if appropriate, and receive an accounting of disclosures by a Business Associate.
- c. Mitigate, to the extent practicable, any harmful effect that is known to UAMS of an impermissible use or disclosure of PHI by its Business Associate.
- d. Covered entities are required to ensure, in whatever reasonable manner deemed effective by the covered entity, the appropriate cooperation by their business associates in meeting these requirements during the transition period.

L. AUTHORITY TO SIGN BUSINESS ASSOCIATE AGREEMENTS: All Business Associate Agreements, or other written contracts evidencing the Business Associate Agreement, must be signed by the UAMS Chief Financial Officer, the UAMS Director of Contract Services, the UAMS Director of Procurement Services, or their designee, whichever is applicable. Applicable signature authority will be determined based upon type of underlying agreement.

All Business Associate Agreements entered in connection with activities of any of the UAMS Area Health Educations Centers (AHECs) also may be signed by the UAMS Executive Director or Associate director of the UAMS AHEC Program.

An original of the executed Agreement should be provided to the UAMS Contract Services Office or Procurement Services Office for the purpose of maintaining a log of all Business Associate Agreements entered into by UAMS.

NO UAMS EMPLOYEE, FACULTY OR STAFF MEMBER IS AUTHORIZED TO EXECUTE A UAMS

BUSINESS ASSOCIATE AGREEMENT, OTHER THAN THOSE INDIVIDUALS LISTED ABOVE.



UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.15
DATE: 03/05/2002
REVISION: 08/15/2005

SECTION: ADMINISTRATION
AREA: GENERAL ADMINISTRATION
SUBJECT: CONFIDENTIALITY POLICY

SCOPE

UAMS physicians, faculty, employees, students, contract personnel, vendors, volunteers, and official visitors.

DEFINITIONS

Confidential Information includes information concerning UAMS research projects, confidential employee information, information concerning the UAMS research programs, proprietary information of UAMS, and sign-on and password codes for access to UAMS computer systems. Confidential information shall include Protected Health Information.

Protected Health Information (PHI) means information that is part of an individual's health information that identifies the individual or there is a reasonable basis to believe the information could be used to identify the individual, including demographic information, and that (i) relates to the past, present or future physical or mental health or condition of the individual; (ii) relates to the provision of health care services to the individual; or (iii) relates to the past, present, or future payment for the provision of health care services to an individual. This includes PHI which is recorded or transmitted in any form or medium (verbally, or in writing, or electronically). PHI excludes health information maintained in educational records covered by the federal Family Educational Rights Privacy Act and health information about UAMS employees maintained by UAMS in its role as an employer.

To access any other terms or definitions referenced in this policy: <http://hipaa.uams.edu/DEFINITIONS%20-%20HIPAA.pdf>

POLICY

UAMS prohibits the unlawful or unauthorized access, use or disclosure of confidential and proprietary information obtained during the course of employment or other relationship with UAMS. As a condition of employment, continued employment or relationship with UAMS, UAMS workforce shall be required to sign the UAMS Confidentiality Agreement approved by the UAMS Office of General Counsel. UAMS will provide training for each of its workforce members on the importance of maintaining confidentiality and the specific requirements of state and federal law, including the HIPAA Privacy Regulations and laws protecting the privacy of students and employees.

This policy applies to information maintained or transmitted in any form, including verbally, in writing, or in any electronic form.

PROCEDURES:

1. **Confidentiality Agreement:** As a condition of employment, continued employment, or a relationship with UAMS, UAMS will require such individuals to sign the UAMS Confidentiality Agreement approved by the UAMS Office of General Counsel. The Confidentiality Agreement shall include an agreement that the signing party will abide by the UAMS policies and procedures and with federal and state laws, governing the confidentiality and privacy of information.

All new employees, students, or vendors requiring access to electronic Confidential Information (computer systems) must have a current Confidentiality Agreement on file in the IT Security Office. The UAMS IT Security Office will maintain signed Confidentiality Agreements and furnish a copy to the individual signing the agreement. It is the responsibility of the manager hiring individual vendors or consultants or receiving sales representatives or service technicians (who do not require electronic access but who may have access to Confidential Information) to require execution of the appropriate confidentiality agreements approved by the UAMS Office of General Counsel and to send those documents to the UAMS IT Security Office.

2. **Restriction on Access, Use and Disclosure of Confidential Information:** UAMS limits and restricts access to Confidential Information and computer systems containing Confidential Information based upon the specific duties and functions of the individual seeking or requiring access. UAMS will restrict access to Confidential Information to the minimum necessary to perform individual job functions or duties. UAMS will further limit and control access to its computer systems with the use of sign-on and password codes issued by the IT Security Office to the individual user authorized to have such access.

Authorization to access, use or disclose Protected Health Information also is governed by the UAMS Use and Disclosure Policy. UAMS will control and monitor access to Confidential Information through management oversight, identification and authentication procedures, and internal audits. UAMS managers and heads of departments will have the responsibility of educating their respective staff members about this Policy and the restrictions on the access, use and disclosure of Confidential Information, and will monitor compliance with this Policy.

3. **Sales Representatives and Service Technicians:** Must register in the appropriate area (Refer to UAMS Guidelines for Vendors and Sales Representatives Policy), sign and complete the Confidentiality Agreement prior to any exposure to UAMS Confidential Information.
4. **Media:** All contacts from the media regarding any Confidential Information must be referred to the UAMS Office of Communications and Marketing (501-686-8998 or pager 501-395-5989)
5. **Violation of Confidentiality Policy:** Individuals shall not access, use, or disclose Confidential Information in violation of the law or contrary to UAMS policies. Each individual allowed by UAMS to have access to Confidential Information must maintain and protect against the unauthorized access, use or disclosure of Confidential Information. Any access, use or disclosure of Confidential Information in any form – verbal, written, or electronic – which is inconsistent with or in violation of this Policy may result in disciplinary action, including but not limited to, immediate termination of employment, dismissal from an academic program, loss of privileges, or termination of relationship with UAMS.

All UAMS employees and others subject to this Policy must report any known or suspected incidents of access, use or disclosure of Confidential Information in violation of this Policy or in violation of the law.

CONFIDENTIALITY AGREEMENT

As a condition of my employment, continued employment or relationship with UAMS, I agree to abide by the requirements of the UAMS Confidentiality Policy and with federal and state laws governing confidentiality of a patient's Protected Health Information, and I agree to the terms of this Confidentiality Agreement.

I understand and agree that if I access, use or disclose Confidential Information in any form – verbal, written, or electronic – in a manner that is inconsistent with or in violation of the Confidentiality Policy, UAMS may impose disciplinary action, including but not limited to, immediate termination of employment, dismissal from an academic program, loss of privileges, or termination of relationship with UAMS.

I understand that when I receive a sign-on code to access the UAMS Network and Systems, I have agreed to the following terms and conditions:

- The sign-on and password codes assigned to me are equivalent to my signature, and I will not share the passwords with anyone.
- I will be responsible for any use or misuse of my network or application system sign-on codes.
- I will not attempt to access information on the UAMS Network and Systems except to meet needs specific to my job or position at UAMS.

I acknowledge that I have read the terms of this Confidentiality Agreement, and that I have received a copy.

_____ SS# _____
(Signature)

Print Full Name: _____

Date: _____ Department: _____

Witness at UAMS Orientation only, otherwise not required: _____

Supervisor/Manager's Signature: _____ Date: _____

(If Vendor, then Department Head Signature required)

Department Head Signature: _____ Date: _____

(Please return completed form to UAMS IT Security Office, #802)

FOR NON-UAMS EMPLOYEES, VENDORS & CONSULTANTS ONLY

Please provide the following additional information:

1. UAMS Sponsor Name/Title: _____

Department: _____

2. What type of access is needed: _____ On-Site _____ Remote

Describe: _____

3. Please describe why the access is needed: _____



UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.39
DATE: 11/01/03
REVISION: 03/01/04

SECTION: ADMINISTRATION
AREA: GENERAL ADMINISTRATION
SUBJECT: CREATION or REVISION of UAMS POLICIES INVOLVING HIPAA ADMINISTRATIVE, SECURITY or PRIVACY REQUIREMENTS

SCOPE

UAMS Workforce

PURPOSE

To establish a system to review, prior to the final approval and publication, UAMS policies developed or revised after April 14, 2003 which involve, impact or affect the administrative, security and privacy requirements of HIPAA.

DEFINITIONS For purposes of this policy, the following definitions apply:

HIPAA means the Health Insurance Portability and Accountability Act of 1996, as amended, and the HIPAA regulations promulgated by the United States Department of Health and Human Services and published at 45 Code of Federal Regulations, Title A, Subchapter C, Parts 160, 162 (Administrative Requirements and Transaction Code Sets), and 164 (Security and Privacy).

Disclosure means the release, transfer, provision of access to, or divulging of information in any manner (verbally or in writing) by UAMS to persons who are not UAMS employees or students, or to any other person or entity **OUTSIDE** of UAMS.

Protected Health Information (PHI) means information that is part of an individual's health information that identifies the individual or there is a reasonable basis to believe the information could be used to identify the individual, including demographic information, and that (i) relates to the past, present or future physical or mental health or condition of the individual; (ii) relates to the provision of health care services to the individual; or (iii) relates to the past, present, or future payment for the provision of health care services to an

individual. This includes PHI which is recorded or transmitted in any form or medium (verbally, or in writing, or electronically). PHI excludes health information maintained in educational records covered by the federal Family Educational Rights Privacy Act and health information about UAMS employees maintained by UAMS in its role as an employer.

UAMS Workforce means for purposes of this Policy, physicians, employees, volunteers, trainees, visiting faculty, and other persons whose conduct, in the performance of work for UAMS, are under the direct control of UAMS, whether or not they are paid by UAMS.

POLICY

Prior to final approval and publication of any policies which involve, impact or affect the requirements of HIPAA, such policies shall be submitted for review to the UAMS HIPAA Office. The UAMS HIPAA Office shall make any revisions necessary to ensure compliance with the HIPAA regulations and to maintain consistency with other UAMS policies concerning the requirements of HIPAA.

PROCEDURE

A. In General – For All Policies:

1. When creating, developing or revising any UAMS policy, the person or committee in charge of creating, developing or revising such a policy must determine whether the policy has the potential to involve, impact or affect a requirement of HIPAA, including both the Security and Privacy aspects of HIPAA. HIPAA regulates, *for example*, the disclosure of PHI; restrictions on disclosure of PHI; confidentiality of PHI; access to PHI; restriction of access to PHI; use of PHI for marketing, fundraising or research purposes; physical and technical safeguarding of PHI; and protection of the integrity and confidentiality of electronically stored PHI.
2. If the policy has the potential to involve, affect or impact a requirement of HIPAA, or if the person or committee in charge of the policy is unsure whether the policy has the potential to involve, affect or impact a requirement of HIPAA, the policy must be submitted to the UAMS HIPAA Office for review prior to the final approval and publication of the policy.
3. The UAMS HIPAA Office will review the proposed policy and make the revisions necessary to ensure compliance with the HIPAA regulations, and any other security or

privacy laws at issue. If revisions are made by the HIPAA Office, the HIPAA Office will provide the revisions to the appropriate person or chair of the committee submitting the policy. After coordinated review between the HIPAA Office and the originators of the policy to discuss any revisions, the HIPAA Office will forward the final policy to the Office of Vice Chancellor for Finance or other appropriate areas or individuals responsible for publishing the particular policy at issue. A copy of the final policy will be provided to the originators of the policy. The HIPAA Office will include a signed Acknowledgment indicating that the policy has been reviewed by the HIPAA Office and whether revisions were made to the policy.

4. If the Acknowledgment by the UAMS HIPAA Office is not included with the HIPAA-related policy sent to the Office of Vice Chancellor for Finance, the Office of Vice Chancellor for Finance must forward the policy to the UAMS HIPAA Office for review and completion of the Acknowledgment form before the policy can be published.

B. Medical Center Policies:

For policies created, developed or revised for the UAMS Medical Center and submitted to the Hospital Compliance Office for approval, the Hospital Compliance Office shall forward the policies to the UAMS HIPAA Office if the Hospital Compliance Office determines that the policy has or may have the potential to involve, affect or impact a requirement of HIPAA. If the Hospital Compliance Office submitted the proposed policy for review by the UAMS HIPAA Office, a completed and signed Acknowledgment form from the HIPAA Office must be included with the policy before the policy can be published in the UAMS Medical Center policies.

C. College Policies:

For policies created, developed or revised for the UAMS Colleges, such as the College of Medicine, College of Pharmacy, College of Nursing, College of Health Related Professions, and all other UAMS Colleges, policies shall be forwarded to the UAMS HIPAA Office if the College determines that the policy has the potential to involve, affect or impact a requirement of HIPAA. If the College submitted the proposed policy for review by the UAMS HIPAA Office, a completed and signed Acknowledgment form from the HIPAA Office must be included with the policy before the policy can be published.

D. Office of Research Policies:

For policies created, developed or revised for research purposes and submitted to the UAMS Office for Research and Sponsored Programs for approval, the Research Privacy Officer shall forward the policies to the UAMS HIPAA Office if the Research Privacy Officer determines that the policy has or may have the potential to involve, affect or impact a requirement of HIPAA. If

the Research Privacy Officer submitted the proposed policy for review by the UAMS HIPAA Office, a completed and signed Acknowledgment form from the HIPAA Office must be included with the policy before the policy can be published.

E. All Other UAMS Department Policies:

For policies created, developed or revised for all other UAMS Departments, including, but not limited to, the Area Health Education Centers (AHECs), the IT Department, the Office of Human Resources, the Purchasing Office, Business Development and Managed Care, these policies shall be forwarded to the UAMS HIPAA Office if the Department determines that the policy has the potential to involve, affect or impact a requirement of HIPAA. If the Department submitted the proposed policy for review by the UAMS HIPAA Office, a completed and signed Acknowledgment form from the HIPAA Office must be included with the policy before the policy can be published.

F. Acknowledgement:

An example of the Acknowledgment form is included with this policy.



UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.31

DATE: 04/01/03

REVISION: 03/01/04

SECTION: ADMINISTRATION

AREA: GENERAL ADMINISTRATION

SUBJECT: DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION AND LIMITED DATA SET INFORMATION

SCOPE

UAMS Workforce

DEFINITIONS

Data Use Agreement means a written agreement between UAMS and a recipient of Limited Data Set information which establishes the permitted uses and disclosures of such information and certain administrative safeguards to protect the information. The standard UAMS Data Use Agreement is attached to the UAMS [Research Policy, 3.1.27](#).

De-Identified Protected Health Information is any information about a patient that does not identify the patient and with respect to which there is no reasonable basis to believe that the information can be used to identify the patient.

Disclosure means the release, transfer, provision of access to, or divulging of information in any manner (verbally or in writing) by UAMS to persons who are not UAMS employees or students, or to any other person or entity **OUTSIDE** of UAMS.

Healthcare Operations is defined by the HIPAA regulations under 45 C.F.R. § 164.501 and is incorporated herein by reference, and includes the following:

1. Quality assessment and improvement, including outcomes evaluation and development of clinic guidelines; population-based activities relating to improving health, protocol development, case management and case coordination, contacting providers and patients with information about treatment alternatives; and related functions that do not include treatment.
2. Accreditation, certification, licensing or credentialing activities, reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals.
3. Conducting or arranging for medical review, legal services and auditing.
4. Business planning and development related to managing and operating the entity.
5. Business management and general administrative activities, such as fundraising and marketing of services to the extent permitted without authorization, disclosure of PHI in a due diligence review or to resolve internal grievances, and customer service.

Limited Data Set means Protected Health Information that excludes the following information about the patient and about *relatives, employers, or household members of the patient*:

- Names;
- Postal address information, other than town and city, state and zip code;
- Telephone numbers;
- Fax numbers;
- Electronic mail address;
- Social Security numbers;
- Medical Record numbers;
- Health Plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including voice and finger prints; and
- Full face photographic images and any comparable images.

Protected Health Information (PHI) means information that is part of an individual's health information that identifies the individual or there is a reasonable basis to believe the information could be used to identify the individual, including demographic information, and that (i) relates to the past, present or future physical or mental health or condition of the individual; (ii) relates to the provision of health care services to the individual; or (iii) relates to the past, present, or future payment for the provision of health care services to an individual. This includes PHI which is recorded or transmitted in any form or medium (verbally, or in writing, or electronically). PHI excludes health information maintained in educational records covered by the federal Family Educational Rights Privacy Act and health information about UAMS employees maintained by UAMS in its role as an employer.

UAMS Workforce means for purposes of this Policy, physicians, employees, volunteers, trainees, and other persons whose conduct, in the performance of work for UAMS, are under the direct control of UAMS, whether or not they are paid by UAMS.

POLICY

UAMS may use Protected Health Information (PHI) to create De-Identified PHI. UAMS may disclose PHI to a Business Associate with whom UAMS has a Business Associate Agreement to create De-Identified PHI. De-Identified information is exempt from the requirements of the HIPAA regulations and may be disclosed to others. UAMS will determine that PHI has been De-Identified in accordance with the Procedures set forth in this Policy and consistent with the HIPAA regulations. This Policy is not intended to address De-Identified information that may be subject to IRB regulations or other applicable laws.

PROCEDURE

UAMS may determine that information about a patient has been “de-identified” so that the information is NOT individually identifiable health information, only if:

- A.** A person with appropriate knowledge and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable determines that the risk is very small that the information could be used alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is subject of the information and documents the methods and results of the analysis that justify the determination; **or**
- B.** The following identifiers of the patient and the patient’s relatives, employers, or household members of the individual are removed:
- Names
 - Geographic subdivisions smaller than a state
 - All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of 90 or older;
 - Telephone and Fax numbers
 - E-Mail, IP, and URL addresses
 - Social Security Numbers
 - Medical Record Numbers
 - Health Plan Beneficiary Numbers
 - Account Numbers
 - Certificate/license Numbers
 - Vehicle Identifiers and Serial Numbers, including license plate numbers
 - Device Identifiers & Serial Numbers
 - Biometric Identifiers, including finger and voice prints
 - Full Face or other comparable photographic images
 - Any other unique identifying number, characteristic, or code.
- C.** The first 3 digits of a zip code can be retained if publicly available data from the Bureau of the Census indicates that the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people, and the initial three digits of a zip code of all such geographic units containing 20,000 or fewer people is changed to 000. The restricted three digit zip codes that must be changed to 000 are: 036, 059, 063, 102, 203, 556, 692, 790, 821, 823, 830, 831, 878, 879, 884, 890, 893, and future ZIP codes that may be added at a later date.
- D.** After removing the identifiers, the information cannot be released if the UAMS employee has actual

knowledge that the information used alone or in combination with other information could identify an individual. See attached flowsheet for additional guidance.

E. Limited Data Set Information. Prior patient Authorization is not required for the use or disclosure of “Limited Data Set” information as defined in this Policy, as long as a Data Use Agreement is entered with the recipient of the information and the use or disclosure is for one of the following purposes:

1. For the purposes of research; or
2. For the purposes of public health activities (not already allowed under HIPAA and the UAMS Use and Disclosure Policy), such as disease registries maintained by UAMS, private organizations, other universities, or other types of studies undertaken by the private sector or nonprofit organizations for public health purposes); or
3. For the purposes of UAMS Health Care Operations as defined in this Policy and under the HIPAA regulations.

UAMS [*Use and Disclosure of PHI and Medical Records Policy, 3.1.28*](#)

START HERE—[DE IDENTIFICATION FLOW CHART](#) (pdf format)



UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.30

DATE: 04/01/03

REVISION: 03/01/04

SECTION: ADMINISTRATION
AREA: GENERAL ADMINISTRATION
SUBJECT: HIPAA EDUCATION AND TRAINING

SCOPE

UAMS Workforce

DEFINITIONS

UAMS Workforce means employees physicians, volunteers, residents, students, trainees, visiting faculty, and other persons whose conduct, in the performance of work for UAMS, is under the direct control of UAMS, whether or not they are paid by UAMS.

POLICY

UAMS will provide to all UAMS Workforce the appropriate education and training necessary to comply with the HIPAA Regulations, and the UAMS HIPAA-related policies and procedures related to the individual's role and specific job duties at UAMS. See [HIPAA Training Matrix](#) Materials for the mandatory HIPAA training must be approved by the UAMS HIPAA Office.

PROCEDURE

All HIPAA training completed by any of these individuals will be recorded in the UAMS Training Tracker System or manually maintained by the UAMS office assigned to the specific training.

- A. General HIPAA Training:** All Physicians and other Healthcare Professionals with FGP or AHEC provider billing numbers, Fellows and Residents must complete the HCCS HIPAA Intranet Training Module within sixty (60) days of their appointment date. User IDs and Passwords for this training may be obtained by contacting the FGP Compliance Office at (501) 603-1219.

All employees who attend New Employee Orientation will receive HIPAA training, at that time. Employees will be required to sign an Attestation establishing that the employee completed the required training program.

Employees also receive an explanation letter and Attestation on HIPAA policies and procedures with instructions to present to their manager or supervisor for additional training in policies and procedures.

All other employees of UAMS who do not attend Orientation must complete an officially sanctioned UAMS HIPAA training program. Employees are required to sign an attestation establishing that the employee completed the required training program within 30 days of hire date.

All UAMS students will receive HIPAA training instructions as part of Orientation. A completed Review and Acknowledgment of Completion must be signed and returned to the UAMS HIPAA Office #829 within 2 weeks after Orientation.

All Volunteers sponsored by UAMS will receive HIPAA training coordinated through the appropriate Office of

Volunteers and approved by the UAMS HIPAA Office.

All UAMS Official Visitors will receive HIPAA training. The UAMS Sponsor of the Visitor must provide HIPAA training materials and obtain a signed UAMS Confidentiality Agreement from the Visitor.

For all other persons, including affiliated students, refer to the [HIPAA Training Matrix](#)

- B. **Research HIPAA Training:** UAMS workforce working with human subjects for research purposes should complete the HIPAA research training along with the IRB Human Subjects Training. <http://www.uams.edu/orc/Training/Training.htm> This includes the principal investigator, co-investigators and research staff including, but not limited to, research associates, research assistants and study coordinators.
- C. **HIPAA Related Policy and Procedures Training:** It is the responsibility of the individual's supervisor to provide employee training on UAMS HIPAA-related policies and procedures specific to their role. An attestation is required.



UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.27

DATE: 04/01/03

REVISION: 03/01/04

SECTION: ADMINISTRATION

AREA: GENERAL ADMINISTRATION

SUBJECT: HIPAA RESEARCH POLICY (Research alone OR combined with treatment)

SCOPE

All UAMS physicians, faculty, employees and students or other UAMS Workforce members performing research on human subjects (living or deceased), or conducting reviews of Protected Health Information preparatory to research. For research conducted by UAMS workforce members in a non-UAMS physical location, such as Arkansas Children's Hospital, the policies of that institution will apply.

DEFINITIONS

For purposes of this Policy, the following definitions apply:

Database means the compilation of data in any form and maintained in any fashion, and includes, but is not limited to, spreadsheets, tables, or other data repositories maintained in any form. This list is not intended to be all inclusive but, rather, a guideline.

Data Use Agreement is a written agreement between UAMS and the Limited Data Set recipient which establishes the permitted uses and disclosures of such information and certain administrative safeguards to protect the information.

De-Identified Information means information which does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. UAMS may determine that health information is De-Identified if the following identifiers of the individual or of relatives, employers, or household members of the individual, are removed, and UAMS does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is the subject of the information:

- Names;
- All geographic subdivisions small than a state, including street address, city, county, precinct, and ZIP Code;
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of 90 or older;
 - Telephone numbers;
 - Fax numbers;
 - Electronic mail address;
 - Social Security numbers;

- Medical Record numbers;
- Health Plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including voice and finger prints; and
- Full face photographic images and any comparable images.

Designated Record Set means, for purposes of Research, medical records about individuals used, in whole or in part, by or for UAMS to make treatment decisions about individuals, including any treatment information generated in the research context.

Disclosure means the release, transfer, provision of access to, or divulging of information in any manner (verbally or in writing) to persons or entities **OUTSIDE** of UAMS.

Limited Data Set means information that **excludes** the following direct identifiers of the individual **and** of relatives, employers, or household members of the individual:

- Names;
- Street or Postal address information (*other than* town, city, State and zip code);
- Telephone numbers;
- Fax numbers;
- Electronic mail address;
- Social Security numbers;
- Medical Record numbers;
- Health Plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;

- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including voice and finger prints; and
- Full face photographic images and any comparable images.

Pre-Research or Review Preparatory to Research means the review of information or records prior to obtaining patient authorization and consent or prior to obtaining an IRB Waiver of Authorization in which the review is solely to prepare a research protocol, to determine if a research project is feasible, or for similar purposes preparatory to research.

Principal Investigator (PI) or Investigator shall mean the UAMS Principal Investigator, researcher or the research team or study coordinators collectively.

Protected Health Information (PHI) means information that is part of an individual's health information that identifies the individual or there is a reasonable basis to believe the information could be used to identify the individual, including demographic information, and that (i) relates to the past, present or future physical or mental health or condition of the individual; (ii) relates to the provision of health care services to the individual; or (iii) relates to the past, present, or future payment for the provision of health care services to an individual. This includes PHI which is recorded or transmitted in any form or medium (verbally, or in writing, or electronically). PHI excludes health information maintained in educational records covered by the federal Family Educational Rights Privacy Act and health information about UAMS employees maintained by UAMS in its role as an employer.

Research shall mean any research or systematic investigation on living or deceased human subjects (retrospective or prospective) seeking the use of PHI, including research development, testing, and evaluation, designed to contribute to generalizable knowledge. This includes research that is consistent with what the IRB currently reviews under the Common Rule.

Workforce means UAMS physicians, faculty, employees, trainees, students, volunteers and other persons who conduct, in the performance of work for UAMS, is under the direct control of UAMS, whether or not they are paid by UAMS.

POLICY

It is the policy of UAMS to protect the privacy and confidentiality of medical records and information contained in the medical records of persons who are subjects of UAMS Research projects as required by law, including any and all Protected Health Information as defined by the HIPAA Privacy Regulations. Protected Health Information of a Research subject, and the use or disclosure of such information, shall be governed by the UAMS Research Policy and any other applicable UAMS policies.

This HIPAA Research Policy is not intended to replace the applicable legal requirements or UAMS policies concerning compliance with professional ethics, the Common Rule, FDA regulations, or other applicable laws and policies. The Principal Investigator (PI) or Project Director (PD) is responsible for obtaining IRB approval for all Research projects that use human subjects including Research projects that propose the use of an individual's or Research subject's PHI. The PI must have the approval letter from the IRB before the project can begin. Please see IRB policies and procedures and the applicable regulations at <http://www.uams.edu/ora/irb> for the regulations and <https://aria.uams.edu> for submitting a human subjects protocol for review and approval by the IRB.

UAMS Workforce working with human subjects for Research purposes must complete the required HIPAA Research Training along with the IRB Human Subjects Training. <http://www.uams.edu/orc/Training/Training.htm>. This includes

the Principal Investigator, co-investigators and research staff including, but not limited, to research associates, research assistants and study coordinators.

PROCEDURES

A. GENERAL: Protected Health Information can be used or disclosed for Research purposes under the following circumstances and only in accordance with this policy:

1. Authorization: The patient or the patient's Legal Representative has authorized the use or disclosure in accordance with this policy;
2. IRB/Privacy Board Review: An Institutional Review Board (IRB) has approved a Waiver of Authorization;
3. De-Identified Information: The PHI is De-Identified;
4. Limited Data Set: Only Limited Data Set information is used or disclosed, and UAMS enters into a Data Use Agreement with the Limited Data Set recipient prior to disclosure;
5. Pre-Research: UAMS obtains from the researcher representations that the use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research;
6. Deceased Individuals: UAMS obtains from the researcher representations that the use or disclosure is sought solely for research on the PHI of deceased individuals.

B. RESEARCH COVERED BY THIS POLICY

1. This policy applies to all Research by UAMS Workforce that involves the use or disclosure of Protected Health Information regardless of the source of funding of the Research.
2. This policy applies to clinical trials, chart reviews, epidemiological studies, behavioral and social science studies, basic science research studies, and research that involves diagnosing or treating an individual as well as Research that involves neither diagnosis or treatment.
3. This policy applies to all Research activities, which includes, but is not limited to the following:
 - The initial review of PHI for Pre-Research purposes such as to determine the feasibility of a study or to develop a research protocol;
 - Research projects that involve the creation of a Database containing PHI;
 - Research projects that involves the use of PHI from current Research Databases;
 - Research projects that involve the addition of PHI to an existing Research Database;
 - Research projects approved by the IRB that create PHI during the Research project;
 - Research projects approved by the IRB that use existing PHI stored in any form;
 - Recruiting patients to participate in a Research study;

- Enrolling patients into a Research study;
- Research projects with patient/subject authorization and consent;
- Conducting a Research study.

4. This policy applies **all UAMS research activities** that use or seek to use PHI about humans, regardless of the form in which the PHI is maintained (e.g., hard copy or electronic format).

C. USES or DISCLOSURES OF PHI – In General

1. **General Requirements:** UAMS will protect the privacy of Research subjects and their PHI collected during a Research project. UAMS will not use or disclose EXISTING PHI or PHI CREATED DURING A RESEARCH PROJECT, unless one of the following circumstances exist:

- a. The subject signs both (1) a HIPAA Authorization for use and disclosure of PHI using the UAMS HIPAA Research Authorization Form or other form containing all the elements of a legally effective HIPAA authorization; AND (2) the informed consent to participate in research form approved by the IRB as required by UAMS policies.

You must give a copy of the signed Authorization and Informed Consent Forms and the UAMS Notice of Privacy Practices to the research subject. Ask subject to sign Acknowledgment form. See [Notice of Privacy Practices Policy 3.1.21](#)

- b. The IRB grants a waiver to the requirement of obtaining a signed HIPAA Research Authorization Form, or
- c. The IRB approved protocol uses properly De-identified PHI, or
- d. The IRB approved protocol uses the Limited Data Set and the recipient (if recipient is not a member of the UAMS workforce) signs a Data Use Agreement with UAMS (or the entity that maintains the Designated Record Set).

2. **Minimum Necessary Applies:** PHI that is used or disclosed for Research purposes without a HIPAA-compliant Authorization should be limited to the minimum necessary to accomplish the purpose of the Research. [Minimum Necessary Policy, 3.1.25.](#)

D. GRANDFATHERING HIPAA RESEARCH AUTHORIZATION – Ongoing Research at Time of April 14, 2003

UAMS may continue to use and disclose PHI created or received before and after April 14, 2003, for Research purposes if UAMS has obtained or received any one of the following prior to April 14, 2003:

- A HIPAA Research Authorization received prior to April 14, 2003, from the patient to use or disclose their PHI for Research purposes; or
- The informed consent of the patient received prior to April 14, 2003, to participate in the Research; or
- An IRB-approved waiver of informed consent for the Research in accordance with the Common Rule and received prior to April 14, 2003.

This includes permissions, consents or waivers that allowed future unspecified Research.

Exception to Grandfathering – When Authorization Required. If the protocol was approved by the IRB prior to April 14, 2003, but the protocol required that informed consent and subjects would be enrolled after April 14, 2003, a protocol revision must be submitted to the IRB adding a separate HIPAA-compliant Research Authorization or amending the informed consent to include the elements of a HIPAA-compliant Research Authorization for subjects enrolled after April 14, 2003.

E. RESEARCH ON INFORMATION OF A DECEASED PERSON

- 1. General Requirements:** A UAMS HIPAA Research Authorization Form is not required when conducting Research of PHI on the deceased. The information requested, however, should be the minimum necessary to accomplish the purposes of the Research. [Minimum Necessary Policy, 3.1.25](#)
The information requested must be solely for Research on the PHI of decedents and not, for example, for Research of living relatives of decedents. Upon request of UAMS, documentation of the deaths of the study subjects will be provided. No Authorization or alteration or waiver of Authorization by an IRB or Privacy Board is needed for use or disclosure of PHI for Research only on the PHI of deceased persons, if these conditions are met, and the Investigator completes a Certification as described below.
- 2. Certification by Investigator:** A Certification by the Investigator is required in which Investigators must certify in writing the following when requesting PHI on deceased individuals: (1) The investigator seeks use and disclosure of PHI for research on deceased individuals; (2) the investigator will provide proof of death if requested; and (3) the investigator seeks PHI solely for Research and nothing else.

For these purposes, PIs will complete and sign a [Certification for Use and Disclosure of Protected Health Information of Deceased Individuals Form](#) and present it to the custodian of the records being requested before the custodian can release the PHI to the investigator.

F. REVIEW PREPARATORY TO RESEARCH:

- 1. Pre-Research or Review Preparatory to Research** means the review of information or records prior to obtaining patient authorization and consent or prior to obtaining an IRB Waiver of Authorization in which the review is solely to prepare a research protocol, to determine if a research project is feasible, or for similar purposes preparatory to research. For example, a review to design a research study, to formulate hypotheses, or to assess the feasibility of conducting a study.

Note: Preparatory to Research activities may include activities to *identify* prospective Research subjects, but it does not include contacting patients, contacting potential subjects, or recruitment of subjects in any manner.

- 2. Authorization:** A UAMS HIPAA Research Authorization Form or other HIPAA Authorization form is not required when conducting Pre-Research or Review Preparatory to Research.
- 3. Minimum Necessary:** The information requested for review must be the minimum necessary to accomplish the purpose of the Pre-Research. [Minimum Necessary Policy, 3.1.25](#). In addition, a Certification by the Investigator is required as described below.
- 4. Certification by Investigator Required:** When undertaking “Pre-Research” or a “Review Preparatory to Research,” investigators must have a current written certification on file signed by the investigator that includes the following representations:

- a. The PI seeks use or disclosure of PHI solely to review such information as necessary to prepare a Research protocol or similar purposes Preparatory to Research; and
- b. PI shall not remove any PHI from UAMS premises in the course of such review; and
- c. The use or disclosure of PHI is necessary for Research purposes.

For these purposes, PIs must fill out a [Reviews Preparatory to Research Form](#), (please print from Word File Icon located at the top of this document) attached, and submit it to the custodian of the records being requested before the custodian can release the PHI to the investigator. Annual renewals are required. See Paragraph 5 below.

5. Re-Certification Required: On an annual basis, PIs must re-new their individual certifications regarding Reviews Preparatory to Research.

6. PHI May Not Leave UAMS Premises: PHI that is being reviewed for Pre-Research purposes must not leave the UAMS premises in the course of such review.

G. IRB APPROVAL OF RESEARCH

The Principal Investigator (PI) or Project Director (PD) is responsible for obtaining IRB approval for **all Research projects** that use human subjects or which otherwise propose the use of an individual's PHI. The PI must have the approval letter from the IRB before the project can begin. Please see IRB policies and procedures at www.uams.edu/ora/hrac for the regulations and visit <https://aria.uams.edu> for submitting a human subjects protocol for review and approval by the IRB.

H. REQUIRED HIPAA RESEARCH AUTHORIZATION

1. HIPAA Research Authorization vs. Informed Consent for Research

All Research projects that use or create PHI will require subjects to sign the usual IRB-approved Informed Consent to participate in a Research project, AND a form similar to the UAMS HIPAA Research Authorization Form as attached, as long as the form contains all the elements of a legally effective HIPAA authorization. The IRB will look for the usual Informed Consent AND the additional HIPAA Research Authorization (example UAMS HIPAA Research Authorization Form) as required by this policy as criteria for granting final approval for a Research project. Beginning April 14, 2003, if the legally effective HIPAA authorization elements are not present in projects using or creating PHI, then the IRB will cite this as a minor revision prior to granting final approval.

2. HIPAA Research Authorization Combined with Informed Consent for Research

- a. **Combination of UAMS HIPAA Research Authorization Form and Informed Consent Form:** UAMS prefers, but will not require, the HIPAA Research Authorization to be a form separate from the Informed Consent form. The HIPAA Research Authorization and the Informed Consent may be combined.
- b. **UAMS HIPAA Research Authorization Form: Example of HIPAA Research Authorization:**

PIs and PDs shall use nothing less than the elements of the UAMS HIPAA Research Authorization Form, but may modify it to make it more stringent if the project dictates it. Researchers are encouraged to modify the form relative to their Research project, but are not authorized to delete any of the required elements presented in the form. The authorization form **MUST** be submitted to the IRB as an update for approval by expedited review.

I. WAIVER OF HIPAA RESEARCH AUTHORIZATION

1. **Waiver of HIPAA Research Authorization:**

If it would be impractical to re-consent or obtain a UAMS HIPAA Research Authorization Form to do the research project, then the PI can request a waiver of the additional HIPAA Research Authorization as described by this policy. PIs or PDs must submit their requests for a waiver of authorization to the IRB in writing and must include the following explicit protocol elements for the waiver of authorization to be considered by the IRB:

- a. Provide a brief description of the Protected Health Information to be used.
- b. Use the following methods to ensure minimal risk to privacy of individuals:
 - (i) Describe an adequate plan to protect the identifiers from improper use or disclosure.
 - (ii) Describe an adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of Research, unless there is a health or research justification for retaining the identifiers or retentions is required by law.
 - (iii) Assure the IRB in writing that the PHI will not be re-used or disclosed to any other person or entity, except as required by law, for authorized oversight of the Research project, or for other Research as permitted by the HIPAA regulations.
- c. Certify in writing that Research cannot practicably be carried out without the waiver.
- d. Certify in writing that Research cannot practicably be conducted without access or use of the PHI.
- e. The IRB approval letter **MUST** contain the following information if a waiver is granted by the IRB:
 - (i) Name of the IRB and the FWA assurance number.
 - (ii) Date of action.
 - (iii) A statement that the IRB determined that the waiver satisfies all the criteria listed above.
 - (iv) A brief description of the PHI for which use and disclosure has been determined to be necessary for Research by the IRB. (Provided by the PI above).
 - (v) The type of review administered under the Common Rule.
 - (vi) Signature of the chair or chair's designee authorized to sign.

J. **WHEN AUTHORIZATION IS NOT REQUIRED**

1. **HIPAA Research Authorization is NOT Required When Information is De-Identified.**

- a. **De-Identified Information** means information which does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. UAMS may determine that health information is De-Identified if the following identifiers of the individual **and** of *relatives, employers, or household members* of the individual, are removed, and UAMS does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is the

subject of the information:

- Names;
 - All geographic subdivisions smaller than a state;
 - All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of 90 or older;
 - Telephone numbers;
 - Fax numbers;
 - Electronic mail address;
 - Social Security numbers;
 - Medical Record numbers;
 - Health Plan beneficiary numbers;
 - Account numbers;
 - Certificate/license numbers;
 - Vehicle identifiers and serial numbers, including license plate numbers;
 - Device identifiers and serial numbers;
 - Web Universal Resource Locators (URLs);
 - Internet Protocol (IP) address numbers;
 - Biometric identifiers, including voice and finger prints;
 - Full face photographic images and any comparable images; and
 - Any other unique identifying number, characteristic or code.
- b. Requirements for Use/Disclosure:** Prior patient Authorization is not required for the use or disclosure of properly De-Identified information as defined in this Policy. Refer to UAMS [De-Identification Policy, 3.1.31](#) to determine proper de-identification methods. Also refer to UAMS [Request for Data Extract Policy, 3.1.29](#). If the PI or other researcher will receive PHI, prior to its being De-Identified, however, the PI/researcher must submit a research protocol to the IRB that includes a description of the health information sought and an explanation of how the information will be De-Identified.
- c. Codes Used to Re-identify the Information.** UAMS may assign to, and retain with, the De-Identified Information, a code or other means of record re-identification as long as that code is not derived from or related to the information about the individual and is not otherwise capable of being translated to identify the individual. For example, a social security number would not be a permissible “code.” A randomly assigned re-identification code, however, would be permissible because it would not be related to information about the individual. UAMS may not

disclose its method of re-identification or use or disclose its code for other purposes. Any codes used to render the information re-identifiable must be kept confidential and held to the same level of privacy as all other PHI pursuant to the policies and procedures of UAMS and the HIPAA regulations.

2. HIPAA Research Authorization is NOT Required for Use/Disclosure of Limited Data Set Information and As Long As Recipient Signs a Limited Data Set Agreement Prior to Disclosure.

a. Limited Data Set means information that **excludes** the following direct identifiers of the individual **and** of *relatives, employers, or household members* of the individual:

- Names;
- Street or Postal address information (*other than* town, city, State and zip code);
- Telephone numbers;
- Fax numbers;
- Electronic mail address;
- Social Security numbers;
- Medical Record numbers;
- Health Plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including voice and finger prints; and
- Full face photographic images and any comparable images.

If the information is necessary for the Research, the Limited Data Set CAN include:

- Geographic identifiers, such as town, city, county, State, and five-digit zip code
(but not street name, street address, or post office box)
- All elements of dates
- Admission dates
- Discharge dates

- Service dates
 - Date of birth and date of death
 - Age (including 90 or over)
 - Other unique codes or identifiers not listed above as a direct identifier
- b. Requirements for Use/Disclosure:** Prior patient Authorization is not required for the use or disclosure of “Limited Data Set” information as defined in this Policy, as long as a Data Use Agreement is entered with the recipient of the information if the recipient is not a member of the UAMS Workforce and the use or disclosure is for one of the following purposes:
- i. For the purposes of Research; or
 - ii. For the purposes of public health activities (not already allowed under HIPAA and the UAMS [Use and Disclosure of PHI Policy, 3.1.28](#)), such as disease registries maintained by UAMS, private organizations, other universities, or other types of studies undertaken by the private sector or nonprofit organizations for public health purposes); or
 - iii. For the purposes of UAMS Health Care Operations as defined in the UAMS [Use and Disclosure of PHI Policy, 3.1.28](#) and the HIPAA regulations.
- c. Data Use Agreement Required:** If the Limited Data Set information is to be disclosed outside UAMS, a Data Use Agreement must be entered with the recipient of the Limited Data Set information. Please contact the UAMS Research Privacy Officer when a Data Use Agreement is needed. All Data Use Agreements require the signature of the UAMS Research Privacy Officer and the authorized representative of the Limited Data Set recipient *prior to disclosure*.
- d. Minimum Necessary Applies:** The Limited Data Set information being used or disclosed must be the minimum necessary to accomplish the purpose of the Research. UAMS [Minimum Necessary Policy, 3.1.25](#).
- e.** Refer to UAMS [De-Identification Policy, 3.1.31](#) to determine proper use/disclosure of Limited Data Set information, and also refer to the UAMS [Request for Data Extract Policy, 3.1.29](#).

K. USE of PHI in EXISTING DATABASES or CREATING A NEW DATABASE

- 1. Research on Existing Databases:** For use or disclosure of PHI for Research purposes from an existing database maintained by UAMS, UAMS must have one of the following:
- Obtain the required HIPAA Research Authorizations in accordance with this Policy; or
 - Obtain an IRB Waiver of Authorization; or
 - Use or disclose PHI for Pre-Research purposes in accordance with this Policy; or
 - Use or disclose PHI for Research on decedents’ PHI in accordance with this Policy; or
 - Use or disclose only the Limited Data Set information and enter into a Data use Agreement

with the recipient in accordance with this Policy; or

- Use or disclose PHI based on permission obtained prior to April 14, 2003 in accordance with the “Grandfathering” section of this Policy.

2. **Collecting PHI for Sole Purpose of Creating Research Database.** Prior to creating a database containing PHI for the purpose of Research, the PI must seek the patient/subject HIPAA Authorizations required under this policy, or seek a Waiver of Authorization from the IRB as described in this Policy.

L. RECRUITMENT: The IRB must approve all recruitment plans prior to the recruiting activity taking place, and the following are examples:

1. Physicians or their clinical staff may identify potential Research subjects from their own patients and contact the patients directly regarding their own IRB approved Research study.
2. Clinical staff, directly involved in patient care, can inform their patients of Research studies and give the patients contact information about Research studies for which they may qualify.
3. A researcher can provide IRB approved flyers and handouts to other physicians or care providers for an IRB approved Research study. These care providers can hand out the flyers and inform subjects to contact the researcher directly for information about the study.
4. IRB Approved Recruitment advertisements can be posted whereby potential subjects can initiate contact with the researcher.
5. Clinical care providers may send a letter or other type of mailing informing their patients of a Research study and provide contact information for the researcher. Initial contact should always be made by a care provider.
6. A researcher can ask care providers to inform their patients of a potential Research study. The researcher should provide the care provider with a [Recruitment HIPAA Authorization form](#) that the patient completes to give their permission for the Researcher to contact them regarding the study. The care providers ask their patients if they would like to be contacted to learn more about the study, the patient completes the form if interested and the care provider then forwards these forms to the researcher. The researcher may then contact the potential subject.

M. TREATMENT RECORDS AND THE DESIGNATED RECORD SET: A **Designated Record Set** means, for purposes of Research, medical records about individuals used, in whole or in part, by or for UAMS to make treatment decisions about individuals, including any treatment information generated in the research context. Documents containing the subject’s PHI in the course of Research and used in Research to make treatment decisions about the subject should be duplicated and the original record provided to the UAMS Health Information Management (HIM)/Medical Records Department for inclusion in the subject’s medical record.

N. ACCOUNTING FOR DISCLOSURES

1. **Accounting Required:** An accounting for disclosures is a method of documenting and tracking disclosures made by UAMS (both oral and written) of PHI to non-UAMS employees or other persons or entities outside UAMS. An example is an oral or written disclosure of PHI to comply with reporting requirements to the Arkansas Department of Health.

UAMS must account for “Disclosures” as defined herein, and in the HIPAA Privacy Regulations, for disclosures made

without the individual's Authorization, such as:

- a. Disclosures of PHI made under an IRB waiver of authorization; and
- b. Disclosures of PHI for Research on the deceased.

See "Exceptions" below.

2. **Accounting Form:** All such disclosures must be documented and accounted for by the PI who disclosed the PHI, or who is in charge of the project in which the PHI was disclosed, using the **Accounting For Disclosures Form attached to the UAMS [Accounting of Disclosures Policy, 3.1.26](#), or other method of documenting the disclosure, and including the information required in the UAMS [Accounting for Disclosures of PHI Policy, 3.1.26](#).** After completing the Form or documenting the disclosure, the Form or documentation must be provided to the UAMS Health Information Management Department (a/k/a UAMS Medical Records Department), Slot #524. Copies may be maintained by the PI.
3. **Multiple Disclosures to Same Person or Entity:** When multiple disclosures of PHI are made to the same person or entity for a single purpose, the accounting for such disclosures may consist of the information required for an accounting for the first disclosure, plus the number or frequency of disclosures, and the date of the last disclosure during the time period covered by the request.
4. **EXCEPTIONS - Accounting is Not Required:** UAMS is NOT required to account for disclosures of the PHI of individual subjects only if the following can be documented:
 - a. A valid HIPAA Research Authorization Form was signed by the individual who is the subject of the PHI being disclosed prior to the disclosure; or
 - b. Only De-Identified Information is being disclosed pursuant to the [UAMS De-Identification Policy](#); or
 - c. Only Limited Data Set information is being disclosed and a Data Use Agreement was entered into with the recipient of the information, as described in this policy and the [UAMS De-Identification Policy](#).

Please print form from Word File (click icon at the top of document)

UNIVERSITY OF ARKANSAS FOR MEDICAL SCIENCES

HIPAA RESEARCH AUTHORIZATION

STUDY TITLE:

Title

PRINCIPAL INVESTIGATOR:

Name

Address

Phone

CO-INVESTIGATORS:

Name

Address

Phone

STUDY SPONSOR:

Name

The word “you” means both the person who takes part in the research, and the person who gives permission to be in the research. This form and the research consent form need to be kept together.

We are asking you to take part in the research described in the consent form. To do this research, we need to collect health information that identifies you. We may collect the following information from your medical record: *<list specific information that will be recorded>*. This information will be used for the purpose of *<list purpose of study>*. We will only collect information that is needed for the research. Participating in this research study will create the following new health information: *<list information that will be created>*. For you to be included in this research, we need your permission to collect, create and share this information.

We will, or may, share your health information with people at the University of Arkansas for Medical Sciences (UAMS) who help with the research or things related to the research process, such as the study staff, the UAMS Institutional Review Board and the research compliance office at the University of Arkansas for Medical Sciences. *We may share your information with the following researchers outside of the University of Arkansas for Medical Sciences: <list who>*. We may also share your information companies that pay for all or part of the research or who work with

us on the research, such as the Sponsor listed above, or their legally authorized representative, or anyone who might purchase those companies at a later date. Additionally, we may need to share your health information with people outside of UAMS who make sure we do the research properly, such as the Office of Human Research Protections or the Food and Drug Administration. We believe that those involved with research understand the importance of preserving the confidentiality of your health information. However, some of the people outside of UAMS may share your health information with someone else. If they do, the same laws that UAMS must obey may not apply to others to protect your health information.

This authorization to collect, use and share your health information expires at the end of the research.

If you sign this form, you are giving us permission to create, collect, use and share your health information as described in this form. You do not have to sign this form. However, if you decide not to sign this form, you cannot be in the research study. You need to sign this form and the research consent form if you want to be in the research study. We cannot do the research if we cannot collect, use and share your health information.

If you sign this form but decide later that you no longer want us to collect or share your health information, you must send a letter to the person and the address listed by "Principal Investigator" on the first page of this form. The letter needs to be signed by you, should list the "Study Title" listed on this form, and should state that you have changed your mind and that you are revoking your "HIPAA Research Authorization". You will need to leave the research study if we cannot collect and share any more health information. However, in order to maintain the reliability of the research, we may still use and share your information that was collected before the Principal Investigator received your letter withdrawing the permissions granted under this authorization.

During the course of the study, you may be denied access temporarily to certain medical information about you that is study related. However, the Principal Investigator and staff will not automatically deny a request, but will consider whether it is appropriate under the circumstances to allow access. If access is denied during the study, once the study is completed, you will be able to request access to the information again.

If you decide not to sign this form or change your mind later, this will not affect your current or future medical care at the University of Arkansas for Medical Sciences.

SIGNATURE, DATE, AND IDENTITY OF PERSON SIGNING

The health information about _____ can be collected and used by the researchers and staff for the research study described in this form and the research consent form.

Signature: _____

Date: _____

Print name: _____

Relationship to participant: _____

The researcher will give you a signed copy of this form.

UAMS DATA USE AGREEMENT FOR THE LIMITED DATA SET

This Data Use Agreement (“DUA”) is made effective this ____ day of _____, 20__, (“Effective Date”) by and between University of Arkansas For Medical Sciences (“Covered Entity”) with offices at _____, and _____ (“RECIPIENT”), with offices at _____; individually, a “Party” and collectively, the “Parties”.

UAMS is a Covered Entity as defined in the Health Insurance Portability and Accountability Act of 1996, as amended (“HIPAA”); and

UAMS is providing RECIPIENT with a Limited Data Set of Protected Health Information (“PHI”) as defined in HIPAA, thus rendering RECIPIENT a “Limited Data Set Recipient” as defined in HIPAA;

The Parties agree to the provisions of this DUA in order to address the requirements of HIPAA and to protect the interest of both Parties.

1. **DEFINITIONS:** Except as otherwise defined, any terms in this DUA shall have the definitions set forth in HIPAA. In the event of any inconsistency between the provisions of this DUA and mandatory provisions of HIPAA, as amended, the HIPAA definition shall control. Where provisions of this DUA are different than those mandated in HIPAA, but are nonetheless permitted by HIPAA, the provisions of this DUA shall control.
2. **USE OR DISCLOSURE:** RECIPIENT shall have the right to use all PHI provided to it by UAMS for the Research, Public Health or Health Care Operations purposes of:

[INSERT THE “USES OF THE DATA” TO BE PROVIDED BY UAMS TO RECIPIENT.]

and any other purpose in satisfaction of a judgment of a court of law or pursuant to any Federal or State law or regulation applicable to such PHI.

3. **RESTRICTIONS ON USE:** RECIPIENT agrees to not use or further disclose the PHI other than is permitted by this DUA, or as otherwise required by law. RECIPIENT shall use appropriate safeguards to protect the PHI from misuse or inappropriate disclosure and shall prevent any use or disclosure of the PHI other than as provided in this DUA. RECIPIENT shall not attempt to identify the individuals to whom the PHI pertains, or attempt to contact such individuals.
4. **REPORTING:** RECIPIENT shall report to UAMS any use or disclosure of the PHI not provided for in this DUA of which RECIPIENT is or becomes aware. RECIPIENT will take reasonable steps to limit any further such use or disclosure.
5. **TERMINATION:** This Agreement and all obligations hereunder, shall be effective on the Effective Date first set forth above and shall continue as long as RECIPIENT retains the data, unless otherwise terminated by applicable law or regulation. RECIPIENT may terminate this Agreement by returning or destroying the PHI. Should RECIPIENT commit a material breach of this Agreement, which breach is not cured within thirty (30) days after RECIPIENT receives notice of such breach from the Covered Entity, then the Covered Entity may discontinue disclosure of PHI and report the breach to the appropriate Privacy Officer at UAMS.
6. **RECIPIENT AS A COVERED ENTITY:** RECIPIENT acknowledges that if it is, itself, a covered entity as defined in HIPAA, then breach of this DUA will be treated as noncompliance with 45 CFR 164.514(e).

IN WITNESS WHEREOF, the Parties have executed this Data Use Agreement as of the day and year first set forth above.

Covered Entity (Covered Entity)

Limited Data Set Recipient

Signature

Signature

Name

Name

Title

Title

UAMS CERTIFICATION

FOR USE OR DISCLOSURE OF PROTECTED

HEALTH INFORMATION FOR THE PURPOSE OF REVIEW PREPARATORY TO RESEARCH (45 CFR 164.512(i)(1)(ii))

Name(s) and Address(es) of Investigator(s):

Name(s) and Address(es) of Covered Entity(ies) Where Protected Health Information is Located:

In accordance with 45 CFR 164.512(i)(1)(ii), the undersigned investigator(s) hereby certify(ies) that:

1. Said investigator(s) seek the use or disclosure of Protected Health Information (as defined in 45 CFR 164.501) located at the Covered Entity(ies), as defined in 45 CFR 160.102, named above solely to review such information as necessary to prepare a research protocol or for similar purposes preparatory to research;
2. Said investigator(s) shall not remove any Protected Health Information from the Covered Entity(ies) named above in the course of the review (and shall record only de-identified Protected Health Information); and
3. The Protected Health Information located at the Covered Entity(ies) named above is necessary for the research purposes of said investigator(s).

Signature(s) of Investigator(s):

Name

Signature

Date

UAMS CERTIFICATION FOR USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION OF DECEASED INDIVIDUALS (45 CFR 164.512(i)(1)(iii))

Name(s) and Address(es) of Investigator(s):

Name(s) and Address(es) of Covered Entity(ies) Where Protected Health Information is Located:

In accordance with 45 CFR 164.512(i)(1)(iii), the undersigned investigator(s) hereby certify(ies) that:

1. Said investigator(s) seek the use or disclosure of Protected Health Information (as defined in 45 CFR 164.501) located at the Covered Entity(ies), as defined in 45 CFR 160.102, named above solely for research on the Protected Health Information of decedents;
2. Said investigator(s) shall, if requested, provide the Covered Entity(ies) named above with documentation of the death of the individuals for whose Protected Health Information said investigators seek use or disclosure; and
3. The Protected Health Information of decedents located at the Covered Entity(ies) named above is necessary for the research purposes of said investigator(s).

Signature(s) of Investigator(s):

Name

Signature

Date

UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.41

DATE: 04/01/2005

REVISION:

PAGE: 1

SECTION: ADMINISTRATION

AREA: GENERAL ADMINISTRATION

SUBJECT: INFORMATION ACCESS FOR TRANSFERS AND TERMINATIONS

SCOPE

UAMS Workforce with Access to Confidential Information, including Electronic Protected Health Information (ePHI), for any purpose.

DEFINITIONS

Confidential Information includes information concerning UAMS research projects, confidential employee information, information concerning the UAMS research programs, proprietary information of UAMS, and sign-on and password codes for access to UAMS computer systems. Confidential information shall include Protected Health Information.

Electronic protected health information means individually identifiable health information that is:

- Transmitted by Electronic media
- Maintained in Electronic media

Protected Health Information (PHI) means information that is part of an individual's health information that identifies the individual or there is a reasonable basis to believe the information could be used to identify the individual, including demographic information, and that (i) relates to the past, present or future physical or mental health or condition of the individual; (ii) relates to the provision of health care services to the individual; or (iii) relates to the past, present, or future payment for the provision of health care services to an individual. This includes PHI which is recorded or transmitted in any form or medium (verbally, or in writing, or electronically). PHI excludes health information maintained in educational records covered by the federal Family Educational Rights Privacy Act and health information about UAMS employees maintained by UAMS in its role as an employer.

UAMS Workforce means, for purposes of this Policy, physicians, employees, volunteers, trainees, and other persons whose conduct, in the performance of work for UAMS, are under the direct control of UAMS, whether or not they are paid by UAMS.

To access any other terms or definitions referenced in this policy:
<http://hipaa.uams.edu/DEFINITIONS%20-%20HIPAA.pdf>

POLICY

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. (UAMS Confidentiality Policy 3.1.15)
UAMS IT Security processes the termination of all employees in accordance with the UAMS Employee Separation Procedure 4.5.16.

PROCEDURE:

These procedures help ensure the timely disabling of UAMS network and information system account(s) and the removal of physical access to UAMS facilities.

- A.** Departments are responsible for updating employee status (job change or termination) in the UAMS Financial System (SAP) on a timely basis.

- B.** The UAMS Financial System (SAP) will send a list of all UAMS workforce terminations (voluntarily or involuntarily) to IT Security. 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.

- C.** Department supervisors are responsible for reviewing transferring employees' computer access levels and notifying the Department's IT Administrator or the UAMS IT Security Office (either by e-mail, phone call (501-526-6028) or by completing the IT System Access Form) of any computer system access levels that must be maintained, assigned or deactivated.

- D.** Physical access to UAMS facilities after termination or transfer. Please refer to UAMS Administrative Guide 11.1.4 *Key Requests/Transfers* for additional details.
 - 1.** Terminations: Upon separation from UAMS, physical access to UAMS facilities is also terminated. As a part of the clearance procedure, faculty and staff shall return all keys to the Physical Plant Key Officer.
 - 2.** Transferring work force members: Direct key transfers to other employees are not permitted. All keys must be returned to the Physical Plant Key Office by the person to whom they were issued.
 - 3.** The Department of the terminating or separating employee will notify the Physical Plant Key Office if a determination is made that locks need to be re-keyed or combinations changed.



UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.25

DATE: 04/01/03

REVISION: 03/01/04

SECTION: ADMINISTRATION
AREA: GENERAL ADMINISTRATION
SUBJECT: MINIMUM NECESSARY POLICY

SCOPE

UAMS Workforce

DEFINITION

Disclosure means the release, transfer, provision of access to, or divulging of information in any manner (verbally or in writing) by UAMS to persons who are not UAMS employees or students, or to any other person or entity **OUTSIDE** of UAMS.

Minimum Necessary means limiting Protected Health Information to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

Protected Health Information (PHI) means information that is part of an individual's health information that identifies the individual or there is a reasonable basis to believe the information could be used to identify the individual, including demographic information, and that (i) relates to the past, present or future physical or mental health or condition of the individual; (ii) relates to the provision of health care services to the individual; or (iii) relates to the past, present, or future payment for the provision of health care services to an individual. This includes PHI which is recorded or transmitted in any form or medium (verbally, or in writing, or electronically). PHI excludes health information maintained in educational records covered by the federal Family Educational Rights Privacy Act and health information about UAMS employees maintained by UAMS in its role as an employer.

Required by law generally means a requirement in the law that compels an entity to make a use or disclosure of information that is enforceable in a court of law. For example, some state and federal statutes or regulations require hospitals to report certain health information to the Arkansas Department of Health, the Arkansas Department of Human Services, the Arkansas State Medical Board, the Arkansas State Board of Nursing, or the Arkansas Pharmacy Board.

UAMS Workforce means for purposes of this Policy, physicians, employees, volunteers, trainees, and other persons whose conduct, in the performance of work for UAMS, are under the direct control of UAMS, whether or not they are paid by UAMS.

Use means the sharing, employment, application, utilization, examination, or analysis within UAMS.

POLICY

For Protected Health Information (PHI) that is subject to the minimum necessary requirements of the

HIPAA regulations, UAMS will make reasonable efforts to limit the use or disclosure of, and requests for, PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request. This policy is **not** intended in any way to impede access to information necessary to make medical decisions and provide treatment to patients. UAMS health care professionals must have timely and sufficient access to patient information for treatment purposes and will use their professional judgment to determine the minimum necessary patient information required to provide such treatment.

PROCEDURE

- A. Exclusions:** The minimum necessary requirement does **not** apply to any of the following:
1. Disclosures to or requests by a health care provider (outside UAMS) for treatment purposes;
 2. Uses or disclosures made to the individual who is the subject of the information;
 3. Uses or disclosures made pursuant to a valid and HIPAA-compliant authorization signed by the patient or patient's Legal Representative;
 4. Disclosures made to the United States Department of Health and Human Services, or any officer or employee of that Department to whom the authority involved has been delegated;
 5. Uses or disclosures Required by Law; and
 6. Uses or disclosures required for compliance with other applicable laws and regulations.
- B.** UAMS will identify the classes of persons or job titles within the UAMS workforce who need access to PHI to carry out their job responsibilities. UAMS will identify the category or categories of PHI to which these individuals need access, and the conditions appropriate to such access.
- C.** For **Uses** of PHI by UAMS health care professionals for **treatment:** UAMS physicians, nurses or other health care professionals may have access to and use the entire medical record of a patient, as needed, for purposes of treatment of that patient. The UAMS physicians, nurses and other health care professionals will use their professional judgment to determine the minimum necessary PHI needed for purposes of treatment, and will not be precluded from having access to the entire medical record or any other Protected Health Information determined by the health care professional to be needed for this purpose.
- D. All other uses or disclosures** subject to the minimum necessary requirements will be reviewed by persons having an understanding of the UAMS privacy policies and practices, and sufficient expertise to understand and weigh the necessary minimum necessary factors.
1. Except for the uses or disclosures of PHI specifically excluded from the "minimum necessary" rule identified under "exclusions" in this policy, UAMS will only use, disclose, or request an entire medical record when the entire medical record is specifically justified as being reasonably necessary to accomplish the purpose of the use, disclosure, or request.
 2. Authorized levels of access shall be determined by job classifications or functions. In unusual or emergency situations, the classes of persons or job titles of UAMS employees may be re-evaluated to determine if additional access to PHI is needed to carry out job

responsibilities.

3. Although UAMS is not required to rely on the following requests to be the minimum necessary, UAMS workforce may reasonably rely on requests made by:
 - a. public health and law enforcement agencies to determine the minimum necessary information for certain disclosures; or
 - b. other covered entities to determine the minimum necessary information for certain disclosures; or
 - c. a professional who is a member of the UAMS workforce, or is a business associate of UAMS for the purpose of providing professional services to UAMS, if the professional or business associate represents that the information requested is the minimum necessary for the stated purpose; or
 - d. a researcher with appropriate documentation from an Institutional Review Board (IRB) or Privacy Board.
 4. For determination of the minimum amount of PHI necessary for disclosures in connection with research purposes, refer to UAMS [*HIPAA Research Policy, #3.1.27.*](#)
- F. Need-To-Know:** Employees will only access PHI on a need-to-know basis for carrying out their specific job duties.



UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.22
DATE: 10/01/04
REVISION: 3/24/2005

SECTION: INFORMATION TECHNOLOGY
AREA: NETWORK SECURITY
SUBJECT: MITIGATION OF USES/DISCLOSURES IN VIOLATION OF HIPAA

SCOPE

UAMS Workforce with Access to Confidential Information, including Electronic Protected Health Information (ePHI), for any purpose.

DEFINITIONS

Confidential Information includes information concerning UAMS research projects, confidential employee information, information concerning the UAMS research programs, proprietary information of UAMS, and sign-on and password codes for access to UAMS computer systems. Confidential information shall include Protected Health Information.

Electronic protected health information means individually identifiable health information that is:

- Transmitted by Electronic media
- Maintained in Electronic media

Mitigate means the steps taken to lessen the harm or potential harm resulting from an improper use or disclosure of Protected Health information, including electronic Protected Health Information.

Protected Health Information (PHI) means information that is part of an individual's health information that identifies the individual or there is a reasonable basis to believe the information could be used to identify the individual, including demographic information, and that (i) relates to the past, present or future physical or mental health or condition of the individual; (ii) relates to the provision of health care services to the individual; or (iii) relates to the past, present, or future payment for the provision of health care services to an individual. This includes PHI which is recorded or transmitted in any form or medium (verbally, or in writing, or electronically). PHI excludes health information maintained in educational records covered by the federal Family Educational Rights Privacy Act and health information about UAMS employees maintained by UAMS in its role as an employer.

UAMS Workforce means, for purposes of this Policy, physicians, employees, volunteers, trainees, and other persons whose conduct, in the performance of work for UAMS, are under the direct control of UAMS, whether or not they are paid by UAMS.

To access any other terms or definitions referenced in this policy: <http://hipaa.uams.edu/DEFINITIONS%20-%20HIPAA.pdf>

POLICY

UAMS will, to the extent practicable, mitigate any harmful effects that are known to UAMS of a use or disclosure of Protected Health Information, including electronic Protected Health Information by UAMS, its Business Associate or Contractors in violation of the HIPAA regulations or the UAMS policies and procedures relative to the requirements of the HIPAA regulations.

PROCEDURE

- A. When UAMS supervisors, managers or department directors are informed that Protected Health Information (PHI) or electronic Protected Health Information (ePHI) has been improperly used or disclosed, such facts will be communicated to the appropriate UAMS Privacy or Security Officer. The Officer notified will contact the UAMS HIPAA Officer to coordinate the investigation and undertake mitigation efforts. The mitigation process must occur in accordance with the [UAMS HIPAA Compliance Plan](#).
- B. If UAMS determines that PHI or ePHI has been improperly used or disclosed by a member of the UAMS workforce, appropriate disciplinary action will be initiated and documented.
- C. If UAMS determines that PHI or ePHI has been improperly used or disclosed by a Business Associate or Contractor, UAMS will:

1. Investigate the incident;
2. Counsel the Business Associate or Contractor on the incident;
3. Monitor the Business Associate's or Contractor's performance for a reasonable period of time following the incident; and
4. If UAMS determines that the Business Associate or Contractor has not taken appropriate steps to remedy the situation leading to the inappropriate use or disclosure, UAMS will terminate the Business Associate or Contractor relationship. Refer to UAMS [*Business Associate Policy, 3.1.33.*](#)



UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.17

DATE: 10/16/02

REVISION: 10/05/05

SECTION: GENERAL ADMINISTRATION
AREA: ADMINISTRATION
SUBJECT: MOBILE DEVICE SAFEGUARDS

SCOPE

UAMS Physicians, Faculty, Employees and Students

DEFINITIONS

Mobile Devices are defined as Personal Digital Assistants (PDAs), tablets, cellular phones, text pagers, laptop computers, and any other types of mobile devices or media that receive, record or store information and data.

Protected Health Information (PHI) means information that is part of an individual's health information that identifies the individual or there is a reasonable basis to believe the information could be used to identify the individual, including demographic information, and that (i) relates to the past, present or future physical or mental health or condition of the individual; (ii) relates to the provision of health care services to the individual; or (iii) relates to the past, present, or future payment for the provision of health care services to an individual. This includes PHI which is recorded or transmitted in any form or medium (verbally, or in writing, or electronically). PHI excludes health information maintained in educational records covered by the federal Family Educational Rights Privacy Act and health information about UAMS employees maintained by UAMS in its role as an employer.

[To access any other terms or definitions referenced in this policy: UAMS HIPAA](#)

POLICY

All UAMS physicians, faculty, employees, and students who use Mobile Devices to access or record Protected Health Information (PHI) are responsible for the protection of the data. Mobile Device users must take the necessary steps to safeguard that information from unauthorized or improper disclosure in violation of UAMS Policies and Procedures or the HIPAA Regulations.

PROCEDURE

- A. Password Protections:** All persons who use Mobile Devices to access or store PHI are required to use the device's password protection feature and use the automatic time out or password protected screen saver feature if available. PHI must be safeguarded in the event the

Mobile Device is lost, stolen, or otherwise accessible by someone other than the user of the device who is authorized to have access to the PHI.

- B. Repairs:** Before sending a Mobile Device for outside repair, the user must make certain that all PHI has been deleted and erased from storage so that any PHI previously stored in the device is rendered completely inaccessible to service technicians or other persons. In the event access to the PHI is necessary for the repairs to be made, a Business Associate Agreement must be in place with the vendor making the repairs. UAMS [Business Associate](#)

[Policy, 3.1.33.](#)

- C. **Beaming:** If PHI is beamed via an infrared information stream, it is possible for another device to inadvertently pick up the transmission. Beaming should take place in the presence of only two (2) Mobile Devices and should be held less than 4 inches apart for the duration of the transmission.
- D. **Wireless Transmissions:** Security measures required by UAMS must be taken when sending PHI in electronic form. Questions regarding specific security measures required should be directed to the UAMS IT Help Desk at (501) 686-8555. Care must be taken to enter the correct pager/cellular phone number when transmitting PHI in text format.
- E. **Storage:** When not in use, Mobile Devices containing PHI must be stored in a secure manner to prevent access by persons who are not authorized to view the PHI stored in the device.
- F. **Reporting:** If a Mobile Device containing PHI is lost or stolen, it must be reported immediately to the UAMS IT Security Officer by calling (501) 686-8555 and the UAMS Campus Police by calling 686-7777.
- G. **Data Removal:** The Mobile Device user is responsible for deleting 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 PHI from the Mobile Device and any other non-UAMS electronic devices so that the PHI previously stored on the device is rendered inaccessible. Questions regarding data removal should be directed to the UAMS IT Help Desk by calling (501) 686-8555.



UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.21

DATE: 10/31/02

REVISION: 03/01/04

SECTION: GENERAL ADMINISTRATION
AREA: ADMINISTRATION
SUBJECT: NOTICE OF PRIVACY PRACTICES

COPE

UAMS Workforce

DEFINITIONS

Indirect Treatment Relationship: A relationship between a patient and healthcare provider in which:

1. The healthcare provider delivers healthcare directly to the patient based on the orders of another healthcare provider; and
2. The healthcare provider typically provides services or product, or reports the diagnosis or results associated with the healthcare, directly to another healthcare provider, who provides the services or product or reports to the patient.

Protected Health Information (PHI) means information that is part of an individual's health information that identifies the individual or there is a reasonable basis to believe the information could be used to identify the individual, including demographic information, and that (i) relates to the past, present or future physical or mental health or condition of the individual; (ii) relates to the provision of health care services to the individual; or (iii) relates to the past, present, or future payment for the provision of health care services to an individual. This includes PHI which is recorded or transmitted in any form or medium (verbally, or in writing, or electronically). PHI excludes health information maintained in educational records covered by the federal Family Educational Rights Privacy Act and health information about UAMS employees maintained by UAMS in its role as an employer.

UAMS Workforce means for purposes of this Policy, physicians, employees, volunteers, trainees, and other persons whose conduct, in the performance of work for UAMS, are under the direct control of UAMS, whether or not they are paid by UAMS.

POLICY

UAMS patients will be provided the UAMS *Notice of Privacy Practices (Notice)* that describes how UAMS uses and discloses protected health information. It will also include the individual's rights and UAMS' legal duties with respect to protected health information. All UAMS HIPAA covered components shall use the UAMS *Notice of Privacy Practices*. Any modifications to the Notice must be approved by the UAMS HIPAA Oversight

Committee.

PROCEDURE

A. Content of the Notice - The UAMS *Notice of Privacy Practices* conforms to §164.520 of the Health Insurance Portability and Accountability Act.

B. Distribution and publication of the Notice - Each UAMS HIPAA covered component will be responsible for making the UAMS *Notice of Privacy Practices* available to its patients in accordance with the HIPAA regulations.

1. For patients with whom UAMS has a **direct treatment relationship**, UAMS will:
 - a. Provide the *Notice* to the patient no later than the date of the first service delivery after April 14, 2003. Make a good faith effort to obtain the individual's written Acknowledgment that they received the *Notice*. Document the reason if the written Acknowledgment was not obtained.
 - b. Post the *Notice* in a clear and prominent location; and
 - c. Make the *Notice* available at all service delivery sites.
2. The *Notice* will be provided to patients who have an **indirect treatment relationship** and **are** physically present at UAMS. The *Notice* will be available upon request to patients **not** physically present and who have an **indirect treatment relationship** at UAMS. An example of this is: mail-in specimens to the UAMS Clinical Laboratory.
3. 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.
4. The Notice will be prominently posted on all UAMS public websites.
5. The *Notice* will be made available in English and Spanish. Other interpretive accommodations will be provided upon request. Refer to University Hospital [*Interpreters Policy P.S.2.07*](#).
6. An audio version, in Spanish and English, of the [*Notice of Privacy Practices*](#) and Acknowledgment may be accessed by dialing (501) 526-7270 or 866-273-3554 (toll free number).

D. Documentation Requirements: A copy of the *Notice* and each subsequent revision will be retained for six years by the UAMS HIPAA Office.

Acknowledgment of Receipt of Privacy Notice

By signing this form, you are only agreeing that you have received a copy of the UAMS Notice of Privacy Practices.

Patient Signature

Date

Print Legal Representative's Name (if applicable) Legal Representative Signature

If Legal Representative, authority of Legal Representative _____
(such as parent of a minor, court-appointed guardian, administrator of estate of deceased,
attorney-in-fact appointed with power of attorney, or healthcare proxy)

STAFF USE ONLY

We provided the Notice of Privacy Practices and attempted to obtain written

Acknowledgment but acknowledgment could not be obtained because:

Patient or Legal Representative declined to sign the Acknowledgment of Receipt.

Other (please specify) _____

Printed Name of Employee Completing Form Date _____

Signature of Employee Completing Form UAMS Location

EPF Barcode

HIPAA



UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.34
DATE: 04/01/03
REVISION: 03/01/04

SECTION: GENERAL ADMINISTRATION
AREA: ADMINISTRATION
SUBJECT: PATIENT INFORMATION RESTRICTION REQUESTS

SCOPE:

UAMS Physicians, Staff, Faculty, Students and Volunteers

POLICY:

All UAMS patients have the right to request restrictions on the use and disclosure of their Protected Health Information. UAMS is not required to agree to any restriction request. UAMS will not agree to any request to restrict information which UAMS is required by law to use or disclose.

PROCEDURE:

- A. Right to Request Restrictions:** Patients will be advised by UAMS Notice of Privacy Practices that they have a right to request restrictions on the use and disclosure of their Protected Health Information. Specifically, patients have the right to request that UAMS restrict:
1. Uses or disclosures of PHI about the patient to carry out treatment, payment or health care operations of UAMS; or
 2. Disclosures made to family and friends involved in the patient's care.
- B. Requirements for Requesting Restrictions:** The patient's request for restrictions must be in writing and must include the following:
1. A description of the information that is to be restricted;
 2. A statement whether the restriction applies to use, disclosure or both; and
 3. To whom the restrictions will apply.

The form attached to this Policy must be completed and signed by the patient in order to process the request. The patient's request must be approved by a UAMS authorized individual. The patient should be informed that the request, if agreed upon, will apply only to the UAMS clinic or facility with which the patient has submitted the request. If the patient wishes for restrictions to apply to other clinics or facilities of UAMS involved in the patient's care, the patient should be informed that he/she must submit the request form to the individual UAMS clinics or facilities. Although UAMS is not required to inform the patient, UAMS may inform the patient verbally or in writing of a denial of a request submitted in writing and in accordance with this Policy. If the patient is informed verbally of a denial of a restriction request, this should be documented on the form. The completed Form should be maintained in the patient's medical record and a copy sent to the UAMS HIPAA Office, #829.

- C. Emergency Situations:** If UAMS has agreed to a restriction, UAMS may not use or disclose PHI in violation

of the restriction, except that, if the patient is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment, UAMS may use the restricted PHI, or may disclose such information to a health care provider, to provide the treatment to the patient.

D. Ineffective Restrictions: A restriction agreed to by UAMS is not effective to prevent disclosures to:

1. Secretary of the United States Department of Health and Human Services to investigate or determine UAMS' compliance with the HIPAA regulations; or
2. Uses or disclosures required by law for:
 - a. public health activities;
 - b. health oversight activities;
 - c. to report abuse, neglect or domestic violence;
 - d. judicial and administrative proceedings;
 - e. compliance with workers compensation proceedings in which patient has filed a workers compensation claim;
 - f. law enforcement purposes;
 - g. to report a crime in an emergency;
 - h. coroners and medical examiners;
 - i. organ, eye or tissue donation purposes;
 - j. circumstances in which UAMS believes in good faith is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or to the public; or
 - k. correctional institutions or other law enforcement custodial situations.
3. Insurance companies or other third party payors for purposes of payment of health care services provided to the patient.

See UAMS [Uses and Disclosure of PHI and Medical Record Policy, 3.1.28](#) for more information.

E. Termination of Agreed Restrictions: UAMS may terminate its agreement to a restriction if:

1. the patient agrees to or requests the termination in writing;
2. the patient orally agrees to the termination and the oral agreement is documented; or
3. UAMS informs the patient that it is terminating its agreement to a restriction, except that such termination is only effective with respect to PHI created or received after UAMS has informed the patient.

UAMS is not required to abide by the "Termination of Agreed Restrictions" requirements when the restrictions do not apply in emergencies as described in Section E of this Policy, or when the restrictions are ineffective under the HIPAA regulations as described in Section D of this Policy.

For a printable version of the form below, please see the [Patient Request to Restrict Use/Disclosure of Health Information](#) Word document.



UNIVERSITY OF ARKANSAS
FOR MEDICAL SCIENCES

Patient label if available or

Print patient name

and account number

Patient Request to Restrict Use/Disclosure of Health Information
(to be completed with assistance of clinic/facility manager or other designee)

/FACILITY NAME: _____

I request the following restriction on the use or disclosure of my health information:

Describe the information you want restricted:

Check whether you want the information restricted from use by UAMS or disclosure outside of UAMS, or both by checking one of the boxes that apply to your request:

- Do not use this information within UAMS
- Do not disclose this information outside UAMS

Specify the persons or entities you want this restriction applied to:

REQUEST WILL APPLY ONLY TO THIS CLINIC/FACILITY.

IF WISH FOR RESTRICTIONS TO APPLY TO ANY OTHER UAMS CLINIC OR FACILITY, PLEASE CONTACT THE CLINIC/FACILITY AND COMPLETE A RESTRICTION REQUEST FORM.

REQUEST IS SUBJECT TO REVIEW AND MAY NOT BE APPROVED.

Signature of Patient or Legal Representative

Date

Representative, authority of Legal Representative _____
(parent of a minor, court-appointed guardian, administrator of estate of deceased, attorney-in-fact appointed with power of attorney or proxy)

.....
Staff Use Only

3.1.34 PATIENT INFORMATION RESTRICTION REQUESTS

Response to request: agreed to request denied request

Notified Patient: verbally in writing Date: _____

Comments: _____

Signature of UAMS Authorized Personnel

Date

Original in Patient's medical record and send a copy to the UAMS HIPAA Office, #829



UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.32

DATE: 04/01/03

REVISION: 03/01/04

SECTION: ADMINISTRATION

AREA: GENERAL ADMINISTRATION

SUBJECT: PATIENT'S REQUEST TO AMEND MEDICAL RECORDS OR PHI

SCOPE

UAMS Workforce

DEFINITIONS

Designated Record Set means a group of records maintained by or for UAMS in which the records are either:

- the medical and billing records about patients maintained by or for UAMS; or
- records used, in whole or in part, by or for UAMS to make decisions about patients.

For purposes of the term “record” in the definition of Designated Record Set, this includes any item, collection or grouping of information that includes Protected Health Information and is maintained, collected, used or disseminated by or for UAMS.

Protected Health Information (PHI) means information that is part of an individual's health information that identifies the individual or there is a reasonable basis to believe the information could be used to identify the individual, including demographic information, and that (i) relates to the past, present or future physical or mental health or condition of the individual; (ii) relates to the provision of health care services to the individual; or (iii) relates to the past, present, or future payment for the provision of health care services to an individual. This includes PHI which is recorded or transmitted in any form or medium (verbally, or in writing, or electronically). PHI excludes health information maintained in educational records covered by the federal Family Educational Rights Privacy Act and health information about UAMS employees maintained by UAMS in its role as an employer.

UAMS Workforce means for purposes of this Policy, physicians, employees, volunteers, trainees, and other persons whose conduct, in the performance of work for UAMS, are under the direct control of UAMS, whether or not they are paid by UAMS.

POLICY

UAMS patients have the right to request that UAMS amend their Protected Health Information or other records about the patient maintained in a Designated Record Set for as long as the Protected Health Information is maintained in a Designated Record Set.

PROCEDURE

- A. Amendment Requests:** Requests by the patient to amend or correct information maintained in the patient's medical record or other records maintained in the UAMS Designated Record Set must be made in writing and

include a reason to support such a request. Routine requests for amendments or corrections to the patient's contact information or other non-medical information are not required to be in writing, and may be handled according to the appropriate department policy and procedure.

B. Response Time: UAMS must act on a patient's request for an amendment within sixty (60) days after receipt of the request in writing. If UAMS is unable to act on the request within the 60-day period, UAMS may have a one-time extension of not more than thirty (30) additional days, as long as UAMS has informed the individual in writing of the delay, the reasons for the delay, and a date that UAMS will provide a response.

C. Basis for Denial of Request: UAMS may deny the amendment request under any one of the following circumstances:

- UAMS did not create the record. If UAMS determines that the patient has provided a reasonable basis to believe that the originator of the record is no longer available to act on the request, UAMS must consider the request, but the request may be denied for other reasons stated in this Policy.
- The information which the patient requests to be amended is not part of a UAMS Designated Record Set.
- The information which the patient requests to be amended is not otherwise available for inspection by the patient under the HIPAA regulations governing a patient's right to access his/her PHI, 45 C.F.R. § 164.524, such as psychotherapy notes, records that are prohibited by law from being released to the individual, and release of the information may endanger the safety of the individual or another person. See UAMS Use and Disclosure of PHI, and Medical Record Policy regarding when UAMS may deny a patient or a patient's legal representative access to the patient information.
- UAMS determines that the information is accurate and complete.

D. Denial Must Be In Writing: If a request to amend is denied, in whole or in part, UAMS must provide the patient with a written denial within the time allowed, using plain language, and must include the following information:

- the basis for the denial; and
- the patient's right to submit a written statement disagreeing with the denial and how to file such a statement; and
- a statement that, if the patient does not submit a statement of disagreement, they may request that UAMS provide their request for amendment and the denial with any future disclosure of the PHI that is the subject of the amendment; and a description of how the patient may complain to UAMS pursuant to the UAMS complaint procedures by contacting the UAMS HIPAA Office at 4301 West Markham Street, #829, Little Rock, AR 72205, or by calling the HIPAA Office at (501-614-2187), or to submit a complaint to the Secretary of the United States Department of Health and Human Services.

E. Patient's Disagreement With Denial of Request:

1. **Statement of Disagreement:** If UAMS denies all or part of the amendment request, the patient may submit a written statement of disagreement and the basis for such a disagreement. UAMS may reasonably limit the length of a statement of disagreement.
2. **Rebuttal Statement:** UAMS may prepare a written rebuttal to the patient's statement of disagreement. When a rebuttal is prepared, UAMS must provide a copy to the patient who submitted the statement of disagreement.
3. **Record Keeping:** UAMS will identify the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link the patient's request for an amendment, UAMS' denial of the request, the patient's statement of disagreement, if any, and UAMS' rebuttal, if any, to the

designated record set.

4. **Future Disclosures:**

- If a statement of disagreement has been submitted, UAMS will include the material appended in accordance with the record keeping section above, or an accurate summary, with any subsequent disclosure of the PHI that the disagreement relates to.
- If a written statement of disagreement has not been submitted, UAMS must include the patient's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the PHI only if the individual has requested such action.
- When a subsequent disclosure described above is made using a standard transaction that does not permit the additional material to be included with the disclosure, UAMS may separately transmit the material required by this section to the recipient of the standard transaction.

F. Recordkeeping of Amendment Requests/Denials: Except for routine requests to amend demographic and contact information concerning the patient, all patient amendment requests should be submitted to the HIM/Medical Records Department using the UAMS Amendment Request Form. If the patient communicates with the provider directly about an amendment request, the provider may elect to respond verbally to the request at that time; however, if the provider elects to respond to the patient's request at that time, and the request is not a routine request to amend demographic and contact information concerning the patient, the Amendment Request form must be filled out during the patient's visit, and the form must include the provider's response, and the completed form must be forwarded to the HIM/Medical Records department.

All documentation regarding requests to amend, and documentation regarding UAMS' response to the request, must be submitted to the Medical Records Department to retain for a period of at least six (6) years from the date of the documentation.

G. Agreeing to Amendment Request: If UAMS agrees, in whole or in part, to the patient's requested amendment, UAMS will:

1. **Make the appropriate amendment** to the information that is the subject of the request by identifying the records in the Designated Record Set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment. With the exception of demographic information, medical information should never be deleted. Instead, the "amendment" must be made in the form of an addition to the record and as required by Arkansas law. Demographic changes may be made without having to maintain a historical file of the change.
2. **Inform the individual** that the amendment is accepted and obtain their identification of and agreement to have UAMS notify the relevant persons with which the amendment needs to be shared. The acceptance of the amendment is not required to be in writing to the patient.
3. **Inform others:** UAMS will make reasonable efforts to inform and provide the amendment within a reasonable time to:
 - persons identified by the patient as having received PHI about them and needing the amendment; and
 - persons, including business associates of UAMS, that UAMS knows to have the PHI that is the subject of the amendment and who may have relied or could foreseeable rely upon such information to the detriment of the individual.

H. When Amendments Made by Others Outside UAMS: If UAMS is informed by another covered entity of its amendment to a patient's PHI maintained by the covered entity, and UAMS has PHI or other records in its Designated Record Set affected by such amendment, UAMS will amend the PHI in its Designated Record Set accordingly.



Patient label if

available

Request for Amendment of Health Information

Patient Name: _____ Birth Date: _____

Patient Account Number: _____ Phone: _____

Patient Address: _____

Date of entry to amend: _____ Type of entry to amend: _____

-

Explain how entry is incorrect or incomplete. What should the entry say to be more accurate or complete?

Identify persons who have received health information about you whom you agree need notice of this amendment, if amendment accepted. Please specify the name and address:

(UAMS will identify others whom it knows have health information that need amendment and document such notice.)

Signature of Patient or Legal Representative

Print Name of Legal Representative

Date _____

-

If Legal Representative, authority of Legal Representative _____

(such as parent of a minor, court-appointed guardian, administrator of estate of deceased, attorney-in-fact appointed with power of attorney, or healthcare proxy)

.....

Staff Use Only

Date request received: _____ Amendment: _____ Accepted _____ Denied

Patient Notified on: _____ (must be within 60 days of request). If denied, notify in writing.

Patient Notified by _____ (name).

If denied, check reason for denial: _____ PHI was not created by this organization

_____ PHI is accurate and complete _____ Other reason (describe): _____

Comments, if any: _____

Signature of UAMS Authorized Personnel

Date

Printed Name

-

[Request for Amendment of Health Information Form](#) (Word format)



UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.35
DATE: 04/01/03
REVISION: 3/1/2004

SECTION: GENERAL ADMINISTRATION
AREA: ADMINISTRATION
SUBJECT: POLICY ON USE OF PHI FOR FUNDRAISING

SCOPE

UAMS physicians, employees, volunteers, trainees, and other persons whose conduct, in the performance of work for UAMS, is under the direct control of UAMS, whether or not they are paid by UAMS.

PURPOSE

To establish guidelines and restrictions for the use and disclosure of Protected Health Information in connection with all UAMS fundraising activities.

DEFINITIONS

For purposes of this policy, the following definitions apply:

Demographic Information shall be limited to the following types of information: (a) the patient's name, address, and other contact information; (b) age; (c) gender; and (d) insurance status.

Fundraising means any activity relating to the efforts of raising funds for the institution of UAMS and its related healthcare facilities.

Protected Health Information (PHI) means information that is part of an individual's health information that identifies the individual or there is a reasonable basis to believe the information could be used to identify the individual, including demographic information, and that (i) relates to the past, present or future physical or mental health or condition of the individual; (ii) relates to the provision of health care services to the individual; or (iii) relates to the past, present, or future payment for the provision of health care services to an individual. This includes PHI which is recorded or transmitted in any form or medium (verbally, or in writing, or electronically). PHI excludes health information maintained in educational records covered by the federal Family Educational Rights Privacy Act and health information about UAMS employees maintained by UAMS in its role as an employer.

POLICY

UAMS may not use or disclose a patient's Protected Health Information (PHI) for Fundraising purposes except as allowed by federal and state law, including the Federal HIPAA Privacy Regulations. UAMS will include an opt-out provision in its Fundraising materials to instruct the recipient on how to opt out of receiving future communications relating to Fundraising.

PROCEDURES

- A. Information Which Can Be Used/Disclosed for Fundraising:** UAMS may use, or disclose to a business associate or to an institutionally related foundation, the following information about the patient for the purpose of raising funds for the benefit of UAMS, without the patient's prior authorization or consent:

- Name
- Address
- Other contact information
- Age
- Gender
- Insurance status
- Dates of healthcare services provided to patient

UAMS may also use the following information for Fundraising purposes:

- public information
- information obtained outside UAMS
- information provided voluntarily by the patient to a member of UAMS' fundraising staff and the patient is aware that it is a member of the UAMS fundraising staff.

- B. Authorization Required for Use/Disclosure of PHI for Fundraising:** Except for the information listed above, no other PHI may be used or disclosed by UAMS for Fundraising purposes, without the patient's signed authorization. The authorization must be an approved UAMS Authorization form allowing the use or disclosure of PHI for fundraising purposes.

Information about the department in which the patient received services also cannot be used or disclosed for Fundraising purposes without the patient's prior authorization, if that information would reveal or could reveal the patient's treatment, diagnosis, or nature of healthcare services. For example, UAMS may not use or disclose for Fundraising purposes the fact that the patient received services from the Department of Psychiatry, the Department of Obstetrics, or the Department of Radiation Oncology.

Examples of PHI which cannot be used or disclosed for Fundraising purposes:

- Diagnosis
- Nature of services
- Treatment
- Place within UAMS where patient received services that specifically identifies the patient's diagnosis, nature of services or treatment received, such as:
 - Department of Psychiatry
 - Department of Obstetrics
 - Department of Radiation Oncology

While UAMS may undertake any Fundraising activities targeted for a specific department or type of illness, UAMS may not use or disclose a patient's PHI to do so (other than as described above in "Information Which Can Be Used/Disclosed for Fundraising").

- C. Opt-Out Provision in Fundraising Materials:** UAMS will include in all Fundraising materials instructions on how the individual may opt out of receiving any future communications relating to Fundraising. An example of

such language would be: “Please write to us at our address if you wish to opt out of future development mailings,” and the address information would be included. UAMS must make reasonable efforts to ensure that individuals who decide to opt out of receiving Fundraising communications are not sent such communications.

- D. Business Associate Agreement:** UAMS will enter into an appropriate Business Associate Agreement pursuant to the UAMS *Business Associate Policy, 3.1.33* prior to disclosing any PHI (including the Demographic Information and dates of healthcare services described above) to an outside consultant or outside entity for Fundraising activities on behalf of UAMS. An institutionally related foundation to whom UAMS discloses PHI for fundraising activities on behalf of UAMS is not considered a “Business Associate” for purposes of this Policy.



UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.24

DATE: 04/01/03

REVISION: 03/01/04

SECTION: ADMINISTRATION
AREA: GENERAL ADMINISTRATION
SUBJECT: PSYCHOTHERAPY NOTES POLICY

SCOPE

UAMS Workforce

DEFINITIONS

Legal Representative means the person authorized by law to act on behalf of the patient, such as the parent of a minor, a court-appointed guardian or a person appointed by the patient in a Power of Attorney document.

Mental Health Professionals include, but are not limited to, psychiatrists, psychologists, licensed social workers, bachelor level social workers, licensed professional counselors or case workers.

Psychotherapy Notes means notes recorded (in any medium) by a health care provider who is a Mental Health Professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the patient's medical record. **Psychotherapy Notes do not include** medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Required by Law means a mandate contained in law that compels UAMS to make a use or disclosure of information and that is enforceable in a court of law. "Required by Law" includes, but is not limited to, court orders and court-ordered warrants, grand jury subpoenas, a governmental or administrative body authorized by law to require the production of the information being sought, Medicare or Medicaid conditions of participation, and statutes or regulations that require the production of the information. "Required by Law" does not mean a subpoena issued by an attorney in a private civil action.

UAMS Workforce means, for purposes of this Policy, employees, volunteers, trainees, and other persons whose conduct, in the performance of work for UAMS, are under the direct control of UAMS, whether or not they are paid by UAMS.

POLICY

All uses and disclosures of Psychotherapy Notes must be in accordance with the federal and state laws and regulations, including the federal HIPAA regulations and consistent with the procedures set forth in this Policy. Psychotherapy Notes are not a part of the patient's medical record and are not required to be disclosed to the patient or the patient's Legal Representative. UAMS will not disclose Psychotherapy Notes to the patient or patient's Legal Representative without prior approval from the originator of the Psychotherapy Notes.

PROCEDURES

- A. Uses and Disclosures of Psychotherapy Notes:** Psychotherapy Notes may be used or disclosed for any of the following purposes:

- Use by the originator of the Psychotherapy Notes for treatment.
- Use or disclosure by UAMS for its own mental health training programs in which students, trainees or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling.
- Use or disclosure by UAMS to defend itself in a legal action or other proceeding brought by the patient who is the subject of the Psychotherapy Notes.
- To investigate or determine compliance with the HIPAA regulations.
- When Required by Law.
- To a health oversight agency in connection with health oversight activities involving the originator of the Psychotherapy Notes.
- To a coroner or medical examiner for the purposes of identifying a deceased person, determining cause of death, or other duties as authorized by law.
- To prevent a serious and imminent threat to the health or safety of a person or the public.

B. Disclosures Requiring Signed Authorization From Patient: For all other uses and disclosures of Psychotherapy Notes, you must obtain (a) the patient's signed Authorization using the UAMS [Authorization for Release of Psychotherapy Notes](#) form; and (b) signed approval from the Mental Health Professional who authored the notes. If the author of the Psychotherapy Notes is no longer employed by or affiliated with UAMS, and there is a reasonable basis to believe that the author is no longer available to act on a request for approval, UAMS may consult another UAMS Mental Health Professional to seek approval for such uses or disclosures of the Psychotherapy Notes still in the possession of UAMS, other than those outlined in the above section.

C. Patient Authorization Must Be Separate Authorization Using UAMS Authorization for Disclosure of Psychotherapy Notes Form: Authorizations for release of Psychotherapy Notes will not be combined with Authorizations for release of other PHI. In the event a patient, or patient's Legal Representative authorized by law to act on behalf of the patient, requests a copy of Psychotherapy Notes or requests the release of Psychotherapy Notes to a third party, UAMS will use the UAMS [Authorization for Disclosure of Psychotherapy Notes](#) form. If there is a request for the release of the patient's PHI at the same time there is a request for the release of Psychotherapy Notes, a separate HIPAA complaint authorization must be provided for the Psychotherapy Notes. UAMS will not provide or accept an authorization that combines the requests into one single authorization.

D. Patient Access and Request for Copies: Psychotherapy Notes are not maintained as a part of the patient's medical record. UAMS is not required to provide patients with access to or a copy of their Psychotherapy Notes. The originator of the Psychotherapy Notes, however, may determine at his or her discretion whether to do so.

E. Security and Storage of Psychotherapy Notes: The Mental Health Professional who is the originator of the Psychotherapy Notes must maintain and store the Psychotherapy Notes in a secure location and manner to preclude unauthorized access or disclosure in violation of this policy or the HIPAA regulations.



UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.18
DATE: 10/16/02
REVISION: 3/01/2004

SECTION: GENERAL ADMINISTRATION
AREA: ADMINISTRATION
SUBJECT: REQUEST FOR ALTERNATIVE METHOD OF COMMUNICATIONS OF PROTECTED HEALTH INFORMATION

SCOPE

All UAMS Physicians, Faculty, Employees, Students and Volunteers

DEFINITIONS

Legal Representative means the person authorized by law to act on behalf of the patient, such as the parent of a minor, a court-appointed guardian or a person appointed by the patient in a Power of Attorney document.

Protected Health Information (PHI) means information that is part of an individual's health information that identifies the individual or there is a reasonable basis to believe the information could be used to identify the individual, including demographic information, and that (i) relates to the past, present or future physical or mental health or condition of the individual; (ii) relates to the provision of health care services to the individual; or (iii) relates to the past, present, or future payment for the provision of health care services to an individual. This includes PHI which is recorded or transmitted in any form or medium (verbally, or in writing, or electronically). PHI excludes health information maintained in educational records covered by the federal Family Educational Rights Privacy Act and health information about UAMS employees maintained by UAMS in its role as an employer.

POLICY

All patients or patient's Legal Representatives may request the University of Arkansas for Medical Sciences (UAMS) to utilize alternative methods or alternative locations for the patient or patient's Legal Representative, or any other information from UAMS containing the patient's Protected Health Information (PHI). UAMS will honor requests which UAMS determines to be reasonable, and UAMS does not require the patient to disclose an explanation or reason for such request. If necessary, UAMS will require the patient to identify how payments will be made.

PROCEDURE

- A. Request Form:** All requests for alternative methods (i.e., written or verbal) or locations (i.e., home or office) to receive PHI must be submitted using the attached form signed by the patient or the patient's Legal Representative and must be referenced in the patient's record.
- B. Department-Specific Procedures:** Individual departments and other UAMS components will develop and implement procedures in compliance with this Policy. UAMS Medical Center employees should refer to the UAMS Medical Center Policy [*Request for Alternative Method of Communications of Protected Health Information*](#).

PS.2.10.

EXAMPLES

Examples of requests include, but are not limited to the following:

1. Patient may request to receive mail from UAMS containing the patient's PHI at a work address instead of home.
2. Legal guardian of patient may request communications from UAMS to be sent to adult children instead of incapacitated elderly parent.
3. Patient may request telephone communication be limited to home telephone.

Patient Label if Available OR	REQUEST FOR ALTERNATIVE METHOD OF COMMUNICATION FORM
Print Patient Name	
Patient Account Number	

Please complete this Form to request UAMS to communicate with you by alternative means or at an alternative location. For example: UAMS mail to be sent to a different address other than your home.

I, _____, request you communicate with me as indicated below:

PRINT Patient's First and Last Name

(Print request in space provided)

I understand this request expires on _____. If I wish to extend my request, I must submit another request in writing to:

UAMS HIPAA OFFICE
4301 West Markham St., #829
Little Rock, AR 72205-7199

I understand that requesting this alternative method of communication may interfere with UAMS' ability to contact me in medical emergencies.

I understand and agree that, **if I cannot be located by the alternative method requested**, UAMS may use any available contact information to locate me in the event that (1) UAMS determines there is a medical emergency or similar situation in which my health is at risk if I am not contacted immediately; or (2) if I have not provided adequate information on how payments will be made.

Signature of Patient or Legal Representative

Date

If Legal Representative, authority of Legal Representative

(such as parent of a minor, court-appointed guardian, administrator of estate of deceased, attorney-in-fact appointed with power of attorney, or healthcare proxy)

For verification purposes, please include your date of birth: _____/_____/_____.

Month Day Year

Patient's telephone number (for processing the Request): _____

For Staff Use Only

Verbal Request Approved

Request Denied If not approved, Patient was notified on _____.

UAMS Staff Signature and Date

NOTE: When using HBO/SMS billing systems, if the Patient and Guarantor are not the same, all billing information will continue to go to the Guarantor's address.

EPF Bar Code HIPAA

[Request for Alternative Method of Communication Form](#) (Word document)



UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.20

DATE: 04/01/03

REVISION: 03/01/04

SECTION: GENERAL ADMINISTRATION
AREA: ADMINISTRATION
SUBJECT: RELEASE OF PATIENT DIRECTORY INFORMATION

SCOPE

UAMS Physicians, Faculty, Employees and Volunteers.

POLICY

Unless the patient requests UAMS not to disclose Patient Directory Information, UAMS may provide Patient Directory Information to a person provided that the caller or requesting party specifies the patient name.

1. Patient Directory Information is limited to the following:
 - Patient name
 - Location in the facility
 - One word statement of condition that does not communicate specific medical information about the patient – to be released by UAMS Medical Center Patient Care Team or Office of Communications and Marketing. [*University Hospital and Clinical Programs Professional Nursing Organization Policy Standards, Patient Confidentiality, J.4.*](#)
 - Religious affiliation – only released to members of the Clergy
2. Patients may restrict or prohibit release of their information from the Directory.
3. UAMS may release the patient's religious affiliation, if given to UAMS by the patient, only to members of the Clergy. Members of the Clergy do not have to specify patient name to request Patient Directory Information. Clergy requests for a list of patients by denomination will be handled by the Office of Pastoral Care at (501) 686-5410.
4. Members of the media who request Patient Directory Information will be referred to the UAMS Office of Communications and Marketing, (501) 686-8149 or (501) 395-5989 in accordance with [*Media Relations and Release of Information, Policy A.2.01.*](#)

UAMS may elect on its own, without a patient's request, to exclude certain patients from the Directory and not release any information. Examples are when the safety/security of patients or others are at risk, or at the request of the UAMS Special Services Office.

PROCEDURE

1. The UAMS workforce should reference the [*UAMS Notice of Privacy Practices Policy*](#) to inform the patients about the information in the Directory and to describe how this information may be disclosed.

2. The **UAMS Notice of Privacy Practices Policy** will inform patients of their rights to omit some or all of their information for directory purposes.
3. The “Request to be Excluded from the Patient Directory” form must be maintained for patients who object to any or all of their information being included in the Directory, or if UAMS determines that the patient should be excluded. UAMS will “flag” directory listings and other applicable records to indicate exclusions have been requested.
4. Requests for a patient condition will be referred to the nursing unit except for requests from members of the media. [Media Relations and Release of Information, Policy A.2.01.](#)
5. Individuals who identify themselves as members of the media will be referred to the UAMS Office of Communications and Marketing.
6. All other requests for Patient Directory information at UAMS Medical Center must be provided via the HBOC Medipac **INFO (Information Desk Inquiry)** screen, the **Patient Information** Screen in OSCAR, by another officially approved mechanism, or by calling Patient Information at (501) 686-6416.
7. If the patient is incapacitated or in an emergency treatment situation, UAMS may use or disclose some or all of the information in the Directory provided the disclosure is:
 - Consistent with a known, prior expressed preference of the patient; and
 - UAMS determines it is in the patient's best interest.

When it becomes practical to do so, UAMS will inform these patients about the uses and disclosures for Directory purposes and offer them the opportunity to decline inclusion in the Directory.

Request to be Excluded from the Patient Directory

If I am a patient at this facility, I understand that the following information in the facility’s Patient Directory is available to any person who asks for me by name:

- (1) my name;
- (2) my location in the hospital or clinic location; and
- (3) a one word statement of my general medical condition (such as good, fair, serious, critical), without any other specific medical information.

I also understand that members of the clergy may receive this information, along with my religious affiliation, even if they do not ask for me by name.

PLEASE COMPLETE ONE OF THE FOLLOWING IF YOU WISH TO RESTRICT THE RELEASE OF INFORMATION ABOUT YOU FROM THE PATIENT DIRECTORY.

I **do not** wish to be included in the Patient Directory. I understand that my exclusion from the Patient Directory will keep this facility from releasing my room number or clinic location to florists, friends, and family and from transferring phone calls to my room. OR

I agree that my name can be listed in the Patient Directory, but I **want to restrict** the release of the following information from the Patient Directory: (check all that apply)

Do not provide my room number or clinic location.

Do not provide a one word statement of condition (such as fair, serious, critical)

Do not provide my religious affiliation

I understand that the above restrictions will apply only to this visit or admission, and that I **must** request restrictions again at future visits if I want any restrictions to be in effect.

Date of admission or clinic visit Signature of patient or representative Today's date

STAFF USE ONLY

Verbal request and the patient or representative was not available to fill out this form.

If a request to exclude information from the Patient Directory is initiated by UAMS, instead of by the patient or a patient's representative, check this box and sign/date below. _____
_____ UAMS employee making the request Date

Patient or UAMS request received and documented in

HBO/OSCAR. _____

_____ UAMS Signature

Date

EPF Barcode

HIPAA



UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.23

DATE: 04/01/03

REVISION: 03/01/04

SECTION: ADMINISTRATION
AREA: GENERAL ADMINISTRATION
SUBJECT: REPORTING OF HIPAA VIOLATIONS

SCOPE

UAMS Workforce

DEFINITIONS

UAMS Workforce means physicians, employees, volunteers, residents, students, trainees, visiting faculty, and other persons whose conduct, in the performance of work for UAMS, is under the direct control of UAMS, whether or not they are paid by UAMS.

POLICY

Any known or suspected violations of the HIPAA regulations or related UAMS policies and procedures must be reported in accordance with this Policy.

UAMS workforce who report in good faith such known or suspected violations shall not be subjected to retaliation, intimidation, discrimination, coercion, or harassment as a result of their report.

Violations of this policy, including failure to report, will be grounds for disciplinary action up to and including termination. Any sanctions that are applied will be documented.

PROCEDURE

Reports by patients or employees may be made to any of the following:

- UAMS Reporting Line (**1-888-511-3639**);
- UAMS HIPAA Office, #829, room number M1/147c, (**501-614-2187**);
- UAMS Research Compliance Office, (**501-526-7134**); or

UAMS IT Security Office (**501-526-6028**).

If the employee making the report is more comfortable reporting to the head of his/her department or anyone else in a position of responsibility, he/she may do so. The person receiving this report should contact the UAMS HIPAA Office as outlined above.

REFERENCES

UAMS [*Clinical Programs Patient Complaint Policy, PS.2.03*](#)



UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.29

DATE: 04/01/03

REVISION: 3/1/2004

SECTION: ADMINISTRATION

AREA: GENERAL ADMINISTRATION

SUBJECT: REQUEST FOR DATA EXTRACTS

SCOPE

UAMS workforce

DEFINITIONS

Disclosure means the release, transfer, provision of access to, or divulging of information in any manner (verbally or in writing) by UAMS to persons who are not UAMS employees or students, or to any other person or entity **OUTSIDE** of UAMS.

Fundraising means any activity relating to the efforts of raising funds for the institution of UAMS and its related health care facilities.

Minimum Necessary means limiting Protected Health Information to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

Protected Health Information (PHI) means information that is part of an individual's health information that identifies the individual or there is a reasonable basis to believe the information could be used to identify the individual, including demographic information, and that (i) relates to the past, present or future physical or mental health or condition of the individual; (ii) relates to the provision of health care services to the individual; or (iii) relates to the past, present, or future payment for the provision of health care services to an individual. This includes PHI which is recorded or transmitted in any form or medium (verbally, or in writing, or electronically). PHI excludes health information maintained in educational records covered by the federal Family Educational Rights Privacy Act and health information about UAMS employees maintained by UAMS in its role as an employer.

UAMS Workforce means for purposes of this Policy, physicians, employees, volunteers, trainees, and other persons whose conduct, in the performance of work for UAMS, are under the direct control of UAMS, whether or not they are paid by UAMS.

POLICY

When a member of the UAMS workforce requests access to any PHI stored electronically concerning a group of patients in order to create a separate database or "data extract" for a use or disclosure permitted by the HIPAA regulations, UAMS will undertake reasonable efforts to limit access to the PHI in the data extract to the Minimum Necessary to carry out the duties of the workforce member or to the amount reasonably necessary to achieve the purpose of the disclosure.

All such uses or disclosures of data extracts containing PHI must be in compliance with UAMS policies, federal and state law, and HIPAA regulations.

UAMS will identify those persons and job titles authorized to perform searches of data to produce and receive data extracts. Periodic audits to determine compliance with this Policy will be conducted.

PROCEDURE

- A.** UAMS Information Technology Department will maintain an inventory of databases containing PHI.
- B.** UAMS workforce members seeking an electronically stored data extract containing PHI must complete a "Request for Data Extract" and submit it to the UAMS custodian of the data who must be authorized by UAMS to perform searches of data to produce extracts. A form is available for your convenience.
- C.** The following information must be included in the request:
1. Name, job title and phone number.
 2. Complete description of data required including time periods, specific search criteria and other information needed from the database.
 3. Entities or individuals for whom the use or disclosure of the PHI is required.
 4. The purpose of the use or disclosure of the data requested.
 5. "Yes" and "no" boxes for the requestor to indicate:
 - a. Is the requestor a Principle Investigator or Research Assistant?
 - b. If the data will be used for research, has an appropriate patient authorization been obtained or has an IRB waiver of authorization been granted?
 - c. If the data requested is to conduct research on deceased individuals, is the [*Certification for Use or Disclosure of Protected Health Information for Deceased Individuals*](#) form current and on file in the UAMS Office of Research and Sponsored Programs.
 - d. If the data is to be used for Review Preparatory to Research, is the [*Certification for Use or Disclosure of Protected Health Information for the Purpose of Review Preparatory to Research*](#) form current and on file in the UAMS Office of Research and Sponsored Programs.
 6. Statement that the requesting party certifies that the information requested is the Minimum Necessary to carry out his or her job duties; or if the request is for a disclosure of PHI, a statement that the requesting party certifies that the information requested is the Minimum Necessary to accomplish the purpose of the disclosure.
 7. Any other information requested by the custodian of the database. A custodian may request completion of a "Request for Data Extract" form.
- D.** If the purpose of the data request is for research or review preparatory to research and the appropriate boxes under (C)(5)(b) through (C)(5)(d) above are not marked "yes," the request must be denied. If the purpose of the data request is a use or disclosure that is not permitted by the UAMS policies, federal or state law, and the HIPAA regulations, the request must be denied.
- E.** Request for Information for Fundraising Purposes: UAMS will use only the following information for Fundraising purposes. See UAMS [*Use and Disclosure of PHI for Fundraising Policy, 3.1.35*](#)
1. a patient's demographic information; and
 2. dates of health care services provided to the patient.

No other PHI may be used or disclosed by UAMS for Fundraising purposes without the patient's signed authorization using the UAMS Authorization for Use/Disclosure of PHI for Fundraising Form.

- F.** The UAMS personnel providing the data extract shall record the date the extract was given to the requesting party and shall maintain a copy of the Request for a minimum of six years from the date of the request.
- G.** UAMS may rely, if such reliance is reasonable under the circumstances, on a requested use as the Minimum Necessary for the stated purpose when the information is requested by a professional who is a member of the UAMS workforce if the professional represents that the information requested is the Minimum Necessary to

carry out his or her job duties; or if the request is for a disclosure of PHI, UAMS may rely on representations from the person requesting the information that the information requested is the Minimum Necessary to accomplish the purpose of the disclosure.

H. For all requests of data extracts containing PHI that will be disclosed outside of UAMS, the UAMS HIPAA Office must approve these requests, including requests by individuals who are not members of the UAMS workforce.

I. Knowledge of a violation or potential violation of this policy must be reported. Refer to UAMS [Reporting Policy for HIPAA Violations, 3.1.23.](#)

J. Disciplinary action may be imposed for accessing, using, or disclosing PHI in violation of this policy.

For a printable version of the form below, please see the [Request for Data Extract](#) Word document.

UAMS REQUEST FOR DATA EXTRACT FORM

All of the information below must accompany all requests for data extracts that contain identifiable patient information.

It is the policy of UAMS to protect the privacy and security of a patient's Protected Health Information (**PHI**).

Requestor's Name _____

Requestor's Job Title _____ Phone # _____

Description of data required (include time periods, specific search criteria, etc.): _____

Entities and/or individuals for whom the use or disclosure of PHI is required: _____

Purpose of the use or disclosure of the requested data: _____

- Is the requestor a Principal Investigator? yes no
- If data will be used for research, has an appropriate patient authorization been obtained or has an IRB waiver of authorization been granted? yes no N/A

If “no”, you must submit the appropriate authorization or waiver before requested data can be released.

- If the data requested is to conduct research on deceased individuals, is the Certification for Use or Disclosure of Protected Health Information of Deceased Individuals form current and on file in the UAMS Office of Research and Sponsored Programs, #636 Yes No N/A
- If data requested is to be used for Review Preparatory to Research, is the Certification for Use or Disclosure of Protected Health Information for the Purpose of Review Preparatory to Research form current and on file in the UAMS Office of Research and Sponsored Programs, #636 Yes No N/A

I am a member of the UAMS workforce and certify that the information requested is the minimum necessary to carry out job duties/accomplish research goals and will be used for the purpose stated above. I am making this request in compliance with the UAMS Minimum Necessary Policy 3.1.25 and, if applicable, with Research Policy 3.1.27.



UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.38

DATE: 10/01/2003

REVISION: July 22, 2005

SECTION: ADMINISTRATION

AREA: GENERAL ADMINISTRATION

SUBJECT: SAFEGUARDING PROTECTED HEALTH INFORMATION

SCOPE

UAMS Workforce with Access to Confidential Information, including Electronic Protected Health Information (ePHI), for any purpose.

DEFINITIONS

Confidential Information includes information concerning UAMS research projects, confidential employee information, information concerning the UAMS research programs, proprietary information of UAMS, and sign-on and password codes for access to UAMS computer systems. Confidential information shall include Protected Health Information.

Electronic Media means:

- (1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as CD-ROM, DVD, floppy disks, magnetic tape or disk, optical disk, or digital memory card; or
- (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

Electronic Protected Health Information (ePHI) means individually identifiable health information that is:

- Transmitted by Electronic media
- Maintained in Electronic media

Information System means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Pre-Research or Review Preparatory to Research means the review of information or records prior to obtaining patient authorization and consent or prior to obtaining an IRB Waiver of Authorization in which the review is solely to prepare a research protocol, to determine if a research project is feasible, or for similar purposes preparatory to research.

Protected Health Information (PHI) means information that is part of an individual's health information that identifies the individual or there is a reasonable basis to believe the information could be used to identify the

individual, including demographic information, and that (i) relates to the past, present or future physical or mental health or condition of the individual; (ii) relates to the provision of health care services to the individual; or (iii) relates to the past, present, or future payment for the provision of health care services to an individual. This includes PHI which is recorded or transmitted in any form or medium (verbally, or in writing, or electronically). PHI excludes health information maintained in educational records covered by the federal Family Educational Rights Privacy Act and health information about UAMS employees maintained by UAMS in its role as an employer.

UAMS Workforce means physicians, employees, volunteers, residents, students, trainees, visiting faculty, and other persons whose conduct, in the performance of work for UAMS, is under the direct control of UAMS, whether or not they are paid by UAMS.

For additional definitions:

<http://hipaa.uams.edu/DEFINITIONS%20-%20HIPAA.pdf>

POLICY

UAMS workforce must undertake appropriate administrative, technical and physical safeguards, to the extent reasonably practicable, to preclude Protected Health Information (PHI) from intentional or unintentional use or disclosure in violation of the HIPAA regulations.

Electronic Protected Health Information (ePHI) and other confidential information located on UAMS Information Systems or Electronic Media must be protected against damage, theft, and unauthorized access. This includes all ePHI and confidential information received, created, maintained and transmitted by UAMS. Confidential information must be consistently protected and managed through its entire life cycle, from origination to destruction. Controls must be in place for hardware and Electronic Media moving into, out of, and within UAMS. Information Systems and Electronic Media for which this policy applies include, but are not limited to, computers (both desktop and laptop), floppy disks, backup tapes, CD-ROMs, zip drives, portable hard drives and PDAs.

PROCEDURE

While access to PHI, and conversations regarding a patient, often must occur freely and quickly in treatment settings, the following safeguards should take place to the extent reasonably practicable:

A. Protecting Printed Information:

1. Route incoming written correspondence through the smallest number of viewers possible.
2. Pre-address all envelopes to individuals or specific departments within UAMS.
3. Keep photocopying of documents containing PHI to a minimum.
4. Shred or place unneeded copies containing PHI in a security bin.
5. Any documents containing PHI should be placed with identifying information face down on counters, desks, and other places where patients or visitors might see them. These documents should not be left out on desks or countertops after business hours and should be placed in locked storage bins, locked desk drawers, or other secure areas.
6. When discarding records or items containing PHI, use a shredder or place the records and items in a bin specifically designated as a shredding bin where the records and items will be retrieved for shredding. All shredding bins should be placed in an area where unauthorized persons cannot easily view or access the PHI contained in the shredding bin.
7. When paper documents are in transit from location to location, place the documents in sleeves, bags, or envelopes that are sealed and clearly addressed to the recipient.

8. When transporting medical records, they should never be left unattended and records should be covered or turned over so that PHI is not visible to casual observers.
9. IV bags and other medically related material that is not suitable for shredding and is placed in regular trash should have all patient identifiers removed or obliterated.
10. Locate fax machines in non-public areas. Refer to UAMS [Faxing of PHI and Other Confidential Information Policy, 3.1.19](#).

B. Bulletin Boards:

Bulletin boards located in areas that may be seen by patients or visitors should not contain any documents containing PHI, unless the patient has agreed to the display by written or documented verbal permission. This would include baby pictures, cards and notes of appreciation and children's signed art work.

C. Storage of Paper-Based Data:

1. After business hours or when not in use by authorized personnel, documents or items containing PHI should be supervised or kept in a locked desk, locked cabinet or other locked location. Storage of documents containing PHI, whether on-site or off-site, must be locked at all times except during use by authorized personnel.
2. Limit the number of keys given to employees. Provide keys to areas and locked cabinets to only those employees whose job responsibilities require or necessitate access to the areas or cabinets where PHI is stored or located.
3. Limit access to filing areas and off-site storage facilities where records or items containing PHI are located to only those employees whose job responsibilities require access to such areas.

D. Shredders:

1. Place shredder machines in a convenient location. If you plan to purchase a shredder, a "cross-cut" shredder is recommended as the security standard.
2. Encourage all staff to use the shredder machines.
3. Shred daily.

E. Outsourcing Shredding:

1. Contract with a reputable vendor.
2. Agree upon acceptable timeframes between pick up and destruction.
3. Review the security of containers in which paper is transported off the site.
4. Monitor the vendor's performance regularly.

G. Physical Security:

1. All persons (patients, visitors, vendors and others) who are not authorized to have access to PHI should

be supervised, escorted or observed when visiting or walking through an area where PHI may be easily viewed or accessed.

2. Utilize a system of controlling the distribution of keys. Require all employees to return all keys upon the effective date of termination of their employment with UAMS, or when the job responsibilities of the employee no longer require access to the areas or cabinets accessed by the key or keys.
3. Doors should be locked at night, unless authorized personnel need access to the rooms or areas after hours.
4. Access to areas containing PHI should be monitored and controlled to the extent possible.

I. Conversations:

1. Conversations with a patient and other conversations in which PHI is being discussed, over the phone or in person, should be made, to the extent possible, in a manner or in a location (or both) where persons who are not intended to be a part of the conversation or who are not authorized to receive the PHI cannot easily overhear the conversation.
2. When having a conversation in a public area with a patient, the patient's family members, or other conversations in which PHI is discussed, conduct the conversation in a lowered voice, to the extent possible, so that unauthorized persons cannot easily overhear the conversation.
3. Avoid using patients' names or the names of patients' family members in public hallways and elevators when persons who are not authorized to receive the information are present.
4. In an emergency situation, where a patient is hearing impaired or in other situations where the ability to discuss PHI quietly and in private may not be practicable, take reasonable precautions to preclude the disclosure of PHI to the extent possible.

J. Paging:

1. Overhead paging of patients and patients' family members should be kept to a minimum. Only request the page if it is urgent and you are unable to locate the patient or family by other means.
2. Only the minimum amount of information should be used when paging. For example, "Mr. John Jones, please return to surgery waiting room."
3. Do **not** request overhead pages for patients who have asked to be omitted from the patient directory.

K. X-Ray Lightboards and Nursing Station Whiteboards:

Place all X-ray lightboards and nursing station whiteboards in an area generally not accessible by the public or readily visible to the public, or implement other safeguards which reasonably limit incidental disclosures to the general public.

L. Sign-In Sheets:

Information on patient sign-in sheets should only include the patient's name and appointment date and time. Do not include unnecessary information such as patient complaint, date of birth, or other information that is not necessary for the sign-in sheet. Use of peel-off labels for patient's to sign, which are then transferred to a sign-in sheet kept outside the view of other patients, is preferable to a sign-in sheet in view of other patients.

M. Charts in Chart Holders Outside Exam Room:

When placing patient records in chart holders outside of examination rooms, turn the records with the front cover facing the wall or with identifying information otherwise covered, so the patient's information is not visible to passersby.

N. Voice Mail/Answering Machine Messages:

1. When leaving a voice mail or answering machine message for a patient, always limit the amount of information disclosed to the minimum necessary, such as the provider name and telephone number, or other information necessary to confirm an appointment, or to ask the individual to call back. For example, when confirming an appointment, the information should be limited to appointment date and time, the doctor's name, and a contact name and telephone number.
2. Do not leave messages that include laboratory and test results, or any other information that links a patient's name to a particular medical condition or the type of clinic or specialist the patient is seeing. (For example, "I am calling to remind Mrs. Brown of her chemotherapy treatment tomorrow at 10:00," is not an appropriate message.)
3. Generally, when leaving a message with a family member or friend answering the patient's phone, the message should be limited to a request for the patient to return your call; and you may leave your name, telephone number, and the fact that you work at UAMS.
4. A patient's verbal permission or written authorization is NOT needed in these circumstances when leaving a message for the patient as directed by this policy and procedure.

O. E-Mail:

All e-mail messages must include a confidentiality statement, including messages sent internally or outside UAMS, and regardless of whether the e-mail message contains PHI. Refer to UAMS [E-Mail Access and Usage Policy, 7.1.12.](#)

P. Faxing:

For documents containing PHI that are faxed internally or outside UAMS, please refer to the UAMS [Faxing Protected Health Information or Other Confidential Information Policy, 3.1.19.](#)

Q. Safeguarding ePHI and other Confidential Information in Electronic Format

1. Access to ePHI is through user authentication and password.
2. Access to Information Systems and Electronic Media containing ePHI and other confidential information at UAMS must be provided only to authorized UAMS workforce members who have a need for specific access in order to accomplish a legitimate task. UAMS workforce members must not attempt to access, duplicate or transmit Electronic Media containing ePHI and other confidential information for which they do not have appropriate authorization. Refer to [Information Access Management Policy, 7.3.04](#) and [Confidentiality Policy, 3.1.15.](#)
3. User access may require specific training depending on the system before access is allowed.
4. UAMS Electronic Storage Media such as, CDs, diskettes and DVDs that contain ePHI should be clearly marked as confidential.
5. UAMS Information Systems and Electronic Media containing ePHI or other Confidential Information should be located and stored in secure environments that are protected by appropriate

security barriers and entry controls.

6. UAMS Information Systems and Electronic Media containing ePHI and other confidential information must be disposed of properly when no longer needed.
 - a. Electronic Media containing ePHI or other Confidential Information that is to be disposed of permanently must be physically destroyed, and may be accomplished in one of the following ways:
 - i. Break diskettes or otherwise render it impossible to re-insert it into a PC drive
 - ii. Punch a hole through the entire diskette
 - iii. Cut CDs into pieces with standard tin-snips
 - iv. Request destruction of CDs and diskettes by a shredding company contracted with UAMS to destroy diskettes and CDs
 - v. Hard drives and tapes are to be destroyed by UAMS IT Department or its designee. Contact UAMS Technical Support with questions regarding disposal.
 - b. Disposal of UAMS Information Systems and equipment containing ePHI must be tracked and logged. At a minimum, such tracking and logging must provide the following information:
 - i. Date of disposal
 - ii. Who performed the disposal
 - iii. Brief description of media or Information Systems that was disposed
 - c. ePHI should be removed from equipment or Information Systems that are being returned to the vendor. If that is not possible, a Business Associate Agreement must be in place before the equipment is returned to the vendor. Contact UAMS Office of Contract Services for more information about Business Associate Agreements.
7. ePHI on UAMS Electronic Media must be removed before such electronic media can be re-used.
8. UAMS Workforce members moving UAMS Information Systems and Electronic Media containing Confidential Information, including ePHI, into, out of, and within the workplace must maintain records of such movement.
9. When necessary, a retrievable, exact copy of data will be created before equipment is moved.
10. ePHI and other confidential information used or sent for Review Preparatory to Research may not be removed from UAMS. Refer to [HIPAA Research Policy 3.1.27](#).
11. ePHI and other confidential information used or sent outside the UAMS Network should be encrypted.

R. Transporting and/or Accessing UAMS Confidential Information off campus for official business use.

1. 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. For employees who work from home part-time or full-time in an official UAMS Capacity refer also to UAMS Administrative Guide [Working from Home Policy 3.1.40](#).
2. The Workforce member is responsible for maintaining the privacy and security of all Confidential Information that they may be transporting, storing or accessing off-site. This includes, but is not limited to:
 - a. Protected Health Information and Electronic Protected Health Information
 - b. Computers that contain or access Confidential Information.
 - c. Printed documents that contain Confidential Information.
3. UAMS policies are in effect whether the Workforce member is working off-site or in a UAMS facility and include the following requirements:
 - a. Electronic media and printed information must be transported and stored in a secure manner.
 - b. The printing of confidential information from home computers should be kept to a minimum and only as needed in accordance with UAMS policies.
 - c. All media containing PHI or ePHI must be disposed of appropriately and must never be placed in regular trash. This includes printed information, faxes, hard drives, diskettes and CDs.
 - d. UAMS materials must be put away when not being used and kept in a secure location that is not accessible to others including children, spouse and visitors.
 - e. Passwords must not be shared or accessible to family members or others
 - f. Any Confidential Information or ePHI sent from workstations, laptops, PDAs and other mobile devices must be encrypted. Refer to [Mobile Device Safeguards Policy 3.1.17](#).
 - g. Anti-virus software must be installed on all home computers and mobile devices used for UAMS business, and they must be password protected.
 - h. Employees are required to maintain updates to current operating systems (ex. Microsoft updates/patches)



UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.28
DATE: 04/01/03
REVISION: 02/07/05
PAGE: 1 of 43

SECTION: GENERAL ADMINISTRATION
AREA: ADMINISTRATION
SUBJECT: USE AND DISCLOSURE OF PHI AND MEDICAL RECORDS POLICY

.PDF FORMS [Authorization For Release Of Information TO UAMS](#)
WITHIN

THIS
DOCUMENT: [Authorization For Release Of Information From UAMS](#)

[Authorization For Release Of Psychotherapy Notes](#)

Please print
form from pdf [Substance Abuse Release information Form](#)

[UAMS Office of Communications Patient Information](#) (photography, video etc.)

TABLE OF CONTENTS

General Information

Verification of Identity/Authority Minimum Necessary Policy

Section 1 – Disclosures to the Patient

Section 2 – For UAMS Treatment, Payment and Operations

Section 3 – To Another Health Care Provider or Covered Entity

Section 4 – Patient Request for Access To or A Copy of Medical Records

Section 5 – Disclosures to Patient’s Legal Representative

Section 6 – Disclosures to Spouse/Family/Friends Involved in Patient’s Care

Section 7 – Patient Authorization Form

Section 8 – Disclosure of Information Outside UAMS for Purposes Unrelated to TPO

Section 9 – Required by Law

Section 10 – Reporting to Agencies or Others Authorized by Law to Receive Information

Section 11 – Court Orders, Warrants and Grand Jury Subpoena

Section 12 – Subpoenas and Discovery Requests from Parties in Litigation

Section 13 – Subpoenas from Law Enforcement Officials

Section 14 – Law Enforcement Generally (Without Court Order or Warrant, Subpoena)

Section 15 – Adult Victims of Abuse, Neglect or Domestic Violence

Section 16 – Adult Victims of Rape, Attempted Rape, Sexual Assault or Incest

Section 17 – Substance Abuse/Treatment Information

Section 18 – Minors

Section 19 – Emergency Circumstances

Section 20 – Patient Request to Amend Record

Section 21 – Costs of Obtaining Copies of Medical Records

Section 22 – Sanctions/Disciplinary Action

SCOPE

UAMS Workforce

DEFINITIONS

Designated Record Set means (i) medical records and billing records; (ii) records used, in whole or in part, to make decisions about patients; and (iii) the enrollment, payment, claims adjudication, and case or medical management record systems.

Disclosure means the release, transfer, provision of access to, or divulging of information in any manner (verbally or in writing) by UAMS to persons who are not UAMS employees or students, or to any other person or entity **OUTSIDE** of UAMS.

Health Care Operations is defined by the HIPAA regulations under 45 C.F.R. § 164.501 and is incorporated herein by reference, and includes the following:

1. Quality assessment and improvement, including outcomes evaluation and development of clinical guidelines; population-based activities relating to improving health or reducing health care costs, protocol development, case management and case coordination, contacting providers and patients with information about treatment alternatives; and related functions that do not include treatment.
2. Accreditation, certification, licensing or credentialing activities, reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals.
3. Conducting or arranging for medical review, legal services and auditing.
4. Business planning and development related to managing and operating the entity.
5. Business management and general administrative activities, such as fundraising and marketing of services to the extent permitted without Authorization, disclosure of PHI in a due diligence review or to resolve internal grievances, and customer service.

Business management and general administrative activities, such as fundraising and marketing of services to the extent permitted without Authorization, disclosure of PHI in a due diligence review or to resolve internal grievances, and customer service.

POLICY

It is the policy of UAMS to protect the privacy and confidentiality of all patient medical records and information contained in the medical records, including the patient's Protected Health Information (PHI), in accordance with applicable state and federal laws and ethical standards. UAMS prohibits persons not authorized by law to obtain access to or copies of a patient's PHI and medical records. UAMS will provide a patient access to, and the right to obtain a copy of, his or her PHI in the patient's Designated Record Set at UAMS for as long as it is maintained in the Designated Record Set and in accordance with this Policy.

Medical records of UAMS patients which are maintained by UAMS, recorded in any form, including data recorded on paper, microfilm, in a computer database or any other medium (e.g., photographs, x-ray films, ECG tracings, videotapes) constitute the property of UAMS. UAMS prohibits the removal of any original medical records from UAMS premises, unless the records are ordered by a court of law or other government authority to be produced in the original form.

A. Verification of Identity/Authority:

1. Identity: In all circumstances, verify the identity of the person to whom you are disclosing PHI, if the person's identity is not known to you, including the identity of the patient. Exception: Patient Directory – If the patient has not opted out of the patient directory, very limited information about the patient may be provided to any person who identifies the patient by name. See "Patient Directory" Section 9 in this Policy, UAMS *Patient Directory Policy, 3.1.20*, and *3.1.37 Verification of Identity Policy 3.1.37* for more information.
2. Authority: Except for the circumstance described above under "Patient Authorization" (when patient has signed Authorization form), verify the authority of the person to request a patient's PHI, or to request that a patient's PHI be disclosed to someone else, if the authority is not known to you. A patient has the authority to request disclosures by virtue of being a patient, and therefore, only a patient's identity must be verified. Refer to Section 9 in this Policy to see elements of a valid HIPAA Authorization.

3. Patient Authorization Using UAMS Authorization Form: If a patient has signed a valid HIPAA authorization or approved UAMS Authorization form to disclose his/her PHI to someone else, then you can follow the Authorization. It is not necessary to verify the authority of the person designated by the patient to receive the information. If a patient's legal representative has signed the UAMS Authorization Form, however, the legal representative's authority must be verified. See "Disclosures to Patient's Legal Representative" and "Patient Authorization Form" set forth in this Policy for more information.

B. Minimum Necessary Policy: All uses and disclosures of PHI must be made in accordance with the UAMS *Minimum Necessary Policy, 3.1.25*.

SECTION 1 – DISCLOSURES TO THE PATIENT – No Patient Authorization Required.

In general, a patient's PHI may be disclosed to the patient, verbally or in writing, without the requirement of any patient authorization. If the patient is not known to you, you must verify the identity of the patient prior to disclosing any information.

Subject to the restrictions and procedures stated in this Policy, a patient has the right to inspect or obtain a copy of their medical records, or PHI maintained in a Designated Record Set, except for the following:

1. Psychotherapy notes as defined in this Policy;
2. Information compiled in, or for use in, a civil, criminal or administrative action or proceeding; or
3. PHI that is subject to the Clinical Laboratory Improvements Amendments of 1988 (CLIA).

See "Patient Request for Access To Or A Copy Of Medical Records" set forth in this Policy for more information.

SECTION 2 – FOR UAMS TREATMENT, PAYMENT AND OPERATIONS – No Patient Authorization Required.

PHI may be used or disclosed without patient authorization for our own Treatment, Payment and Health Care Operations as defined herein. Such use and disclosure, however, is subject to the requirements of the UAMS Minimum Necessary Policy (limiting the use or disclosure of PHI to the minimum necessary) and the UAMS Patient Restriction Request Policy (allowing the patient to restrict the use or disclosure of PHI in certain circumstances). The identity and authority of the person requesting or receiving the PHI must be verified.

SECTION 3 – TO ANOTHER HEALTH CARE PROVIDER OR COVERED ENTITY – No Patient Authorization Required.

A. **To Other Health Care Provider or Covered Entity for Treatment or Payment:** UAMS may disclose a patient's PHI, without patient Authorization, to any other health care provider for the treatment and payment activities of that provider which relate to the patient who is the subject of the PHI disclosed, regardless of whether the health care provider is or is not a Covered Entity.

B. **To Other Health Care Provider or Covered Entity for Operations:** UAMS may disclose PHI, without patient Authorization, to any other provider for health care operations of that provider, regardless of whether the provider is or is not a Covered Entity, only if:

1. the provider either has or had a relationship with the individual who is the subject of the PHI being requested; and
2. the PHI pertains to such relationship; and
3. the disclosure is for the purpose of the provider's health care operations listed in the Definition of "Health Care Operations" described in Parts (1) and (2) this Policy.

- C. **To a Provider in Organized Health Care Arrangement:** In addition to the disclosures allowed to other providers or covered entities as described above, if the provider/covered entity participates with UAMS in an Organized Health Care Arrangement (as defined by HIPAA), UAMS *also* may disclose PHI, without patient authorization, to the provider/covered entity for the purpose of any health care operation activities of the Organized Health Care Arrangement.

SECTION 4 – PATIENT REQUEST FOR ACCESS TO OR A COPY OF MEDICAL RECORDS -- No Patient Authorization Required

A. **General Policy Relating to Patient’s Request for Access To or Copy of Record:**

Subject to the restrictions and procedures stated in this Policy, an adult or emancipated minor patient has the right to inspect or obtain a copy of their medical records, or PHI maintained in a Designated Record Set, except for the following:

- Psychotherapy Notes as defined in this Policy;
 - Information compiled in, or for use in, a civil, criminal or administrative action or proceeding; or
 - PHI that is subject to the Clinical Laboratory Improvements Amendments of 1988 (CLIA).
1. **Viewing or copying of current admission records while an inpatient:** Subject to the requirements of this Policy, nursing staff or clinicians may allow **patients** to view or have a copy of their records as follows:
 - a. Patients may view their **current** admission records, as long as:
 - 1.1 The physician is notified and approves the viewing; and
 - 1.2 The patient has signed a UAMS Authorization form. Although the use of the Authorization form is not required for a patient to view his/her own record, it is the preferred method. UAMS must also accept a written request from the patient, or documentation of such request, and response to the request must be made in the patient’s progress notes.
 - b. Patients may have a copy of their **current** admission records, as long as a written request from the patient is obtained, and documentation of such request and response to the request is made in the progress notes. The patient should be referred to Health Information Management/Medical Records Department to process the patient’s request for copies. The physician should be notified before copying current admission records. The records will be copied according to this Policy and the HIM/Medical Records Department Release of Information policy.
 - c. **NOTE: Physicians and nurses**, using their professional judgment, may provide a patient with a copy of any portion of their records, such as diagnostic results, progress notes, or other records, **without** requiring the patient to obtain the records from HIM/Medical Records Department. In that event, the physician, nurse or other personnel should document in the patient’s progress notes the patient’s request and the records provided.
 2. **Requests for Access/Copy While an Outpatient:** Subject to the requirements of this Policy, if patient requests an outpatient clinic or service area to provide access to or a copy of the patient’s medical record, the clinic or service area may provide access to or a copy of the record to the patient, under the following circumstances:

- a. The patient is requesting only information from the most recent service or diagnostic reports associated with the most recent service; **and**
- b. The patient is requesting information only from that clinical service area; **and**
- c. The patient has provided a written request for the records, or the clinic has made a note in the patient's medical record identifying the records provided to the patient.

Outpatient areas are not to copy or print from any protected health information source from a previous date of service or from a different clinic for release to the patient.

All requests for previous information or information from another clinical service should be forwarded to the Health Information Management/Medical Records Department. Components of UAMS should forward requests to the designated area of their facility.

3. **Never Leave Patient Alone With UAMS Record:** When providing a patient or family member access to the patient's medical record, a designated UAMS employee **must** be present at all times to protect the integrity and confidentiality of the information. Items may not be added to or removed from the medical record.
4. **Questions Regarding Treatment or Amendment of Record:** All questions regarding treatment must be forwarded to the physician. If the patient wants to make an amendment to correct information in his/her medical record, an Amendment Request form must be completed in accordance with UAMS [*Patient's Request to Amend Medical Records or PHI, 3.1.32.*](#)
5. **Viewing or copying of patient's previous medical records:** Refer to Medical Records Department and Written Request Required. If a patient requests access to or a copy of his/her medical records, or PHI maintained in a Designated Record Set, the patient will be referred to Health Information Management/Medical Records Department and the request for such records must be in writing. The records will be copied according to this Policy and the HIM/Medical Records Department Release of Information policy. Requests to review medical records in person require an advance appointment.

Family of Patient Viewing or Having Copy of Medical Record: If the patient is requesting that **family or another designee** view or have a copy of the patient's record while patient is an inpatient or outpatient, an Authorization form **must** be signed by the patient. See the attached Authorization for Access to and Release of Information Form. See also "Disclosures to Spouse/Family/Friends Involved in Patient's Care" section of this Policy.

C. Timeliness of Response to Request for Access To or Copy of Record: UAMS will act on a request for access to or a copy of a medical record within thirty (30) days after receipt of the request if the record is held or is accessible on site, or within sixty (60) days if it is not accessible on site. This time limit may be extended for an additional thirty (30) days if UAMS sends the person a written statement of the reason for the delay and the date when the party can have the information. UAMS should date-stamp the first page of any written request or otherwise indicate when the request was received by UAMS. All written requests and authorizations must be stored in the patient's record. Even if UAMS receives duplicate requests, all such requests must be stored in the patient's record.

1. If the request is granted, in whole or in part, UAMS will inform the requesting party of acceptance and provide the access requested.
2. If the request is denied, in whole or in part, UAMS will provide a written denial to the patient in accordance with this policy.

D. Denial of Access/Copy Without Opportunity to Review: UAMS may deny access to or a copy of PHI without providing an opportunity for the patient or personal representative to review the denial in the following circumstances:

1. The PHI is exempt from right to access as set forth in Section 6A.1 above.
2. An inmate's request to obtain PHI, if obtaining such information would jeopardize the health, safety, security, custody, or rehabilitation of the inmate or other inmates, or the safety of any officer, employee, or other person at the correctional institution or the person transporting the inmate.
3. The PHI was created or obtained during a research study that involves treatment of the patient and the patient agreed not to access the PHI until the study is concluded.
4. If UAMS received the PHI from someone other than a health care provider and promised to keep the PHI confidential and allowing access would be likely to reveal the source of the information.

E. Denial of Access/Copy with Opportunity to Review: In the following circumstances, UAMS may deny access to or a copy of PHI. However, the patient has the right to have the denial reviewed by a licensed health care professional designated by UAMS, who was not involved in the original decision to deny the request.

1. Requests for information that UAMS reasonably believes is likely to cause substantial harm or to endanger the physical safety or life of the patient or another person.
2. Requests made by a personal representative where the access is reasonably likely to cause substantial harm to the patient or another person.

F. Response to Patient if Request to Access/Copy is Denied: UAMS will comply with the following when denying access to PHI:

1. If possible, exclude the parts to which UAMS has grounds to deny access and allow access to the rest of the PHI.
2. Provide a timely written denial to the requesting party containing:
 - a. The basis for the denial;
 - b. A statement of the patient's review rights, including a description of how the patient may exercise such review rights; and
 - c. A description of how the patient may complain to the hospital as specified in its Notice of Privacy Practices or to the Secretary of DHHS.
3. If UAMS does not maintain the records but knows where the information is maintained, UAMS will inform the patient where to direct the request for access.
4. UAMS will refer any request for a review to the designated licensed health care professional who will, within a reasonable time, determine whether or not to uphold the denial.
5. UAMS will promptly provide written notice of the review decision to the patient or take other action as required.

SECTION 5 – DISCLOSURES TO PATIENT'S LEGAL REPRESENTATIVE – No Patient Authorization Required, but Must Be Authorized By Law.

A. Patient's Legal Representative: Except as provided by this Policy, UAMS must treat a patient's Legal Representative as the patient for purposes of the use and disclosure of the patient's PHI. The following determinations must be made in considering whether a person is a Legal Representative authorized by law to act on behalf of the patient:

1. The person is authorized by law to act on behalf of the patient in connection with the patient's health care decisions, such as:
 - a. Parent of their minor child; - See "Minors" Section of this Policy
 - b. Court-appointed Guardian of a minor;
 - c. Court-appointed Guardian of an elderly or incapacitated person;
 - d. Appointed by the patient to act as their attorney-in-fact in a Durable Power of Attorney with health care rights;
 - e. Appointed by the patient in a Health Care Proxy;
 - f. A person authorized by Ark. Code Ann. § 20-9-602 to verbally or otherwise consent to treatment/procedures suggested/directed by physician for the following persons of "unsound mind":
 - 1) adult sibling of the patient of unsound mind; or
 - 2) spouse of the patient of unsound mind; or
 - 3) adult child for parent of unsound mind.
 - g. Court-appointed Administrator or Executor or Personal Representative of the Estate of a deceased patient. A guardianship or a power of attorney (or any other grant of authority by the patient) are no longer effective upon death. No will is effective until probated.
 - h. For persons who are terminally ill or permanently unconscious – see Ark. Code Ann. 20-17-202;
 - i. For Incapacitated persons for whom there is no health care proxy or other authority, see to Ark. Code Ann. 20-17-214.

B. Verification of Identity/Authority: UAMS will request verification of the identity of the Legal Representative, if not known, and the authority of the Legal Representative to act on behalf of the patient, if not known. If no evidence of his/her authority is available in the record or otherwise, such as a copy of the court order, the Power of Attorney or any other written documentation evidencing their authority, UAMS will request a copy from the Legal Representative.

C.

Do Not Provide PHI if Suspected Harm by the Representative: A provider is not required to treat a person as the Legal or Personal Representative of the patient for purposes of disclosing PHI if the provider has a reasonable belief that the patient has been or may be subjected to violence, abuse or neglect by the person acting as a Legal/Personal Representative, or it could endanger the patient, or it is not in the best interest of the patient.

SECTION 6 – DISCLOSURES TO SPOUSE/FAMILY/FRIENDS INVOLVED IN PATIENT'S CARE – No Patient Authorization, but Special Circumstances Must Exist.

- A. Verification of Identity:** The identity of the patient and the person receiving the PHI must be verified. In making verification decisions in these *particular* circumstances, UAMS may rely on the exercise of professional judgment of its staff to determine a person's identity.
- B. When Patient Present (in person or on phone): Can disclose to Spouse, Family or Friends only under the following circumstances:**
1. If the spouse, family or friend is identified by the patient; and
 2. The spouse, family or friend is involved in the patient's care; and
 3. One of the following circumstances exists:
 - a. Patient has agreed (verbally on phone or otherwise); or
 - b. Patient does not object when provided opportunity to do so; or
 - c. You can reasonably infer from circumstances that the patient does not object (such as when patient brings family member into examination room); or
 - d. There is a medical emergency.

PHI disclosed in these circumstances must be limited to PHI that is directly relevant to person's involvement with the patient's care or payment; **or** to notify them of patient's location, one word statement of general condition, or death.

- C. When Patient is NOT Present (in person or on phone), then we may:**
1. Disclose (by phone or otherwise) to spouse/family/friends involved in patient's care PHI that is directly relevant to the person's involvement with the individual's health care or payment if we determine that disclosure is in the best interest of the patient.
 2. Allow person to pick up filled prescriptions, medical supplies, X-rays or other similar forms of PHI, using professional judgment and experience with common practice to make reasonable inferences of the patient's best interest in allowing a person to act on behalf of the individual.
- D. When Patient Cannot Agree/Object Because of Patient's Incapacity or an Emergency Circumstance, then we may:**
1. Disclose [by phone or otherwise] the PHI permitted for the facility directory (name, location and one word statement of general condition), but only if this is consistent with a prior expressed preference of the patient and it is in the patient's best interest to do; and
 2. Disclose [by phone or otherwise] to spouse/family/friends involved in patient's care PHI that is directly relevant to the person's involvement with the individual's health care or payment if we determine that disclosure is in the best interest of the patient; and
 3. Allow person to pick up filled prescriptions, medical supplies, X-rays or other similar forms of PHI, using professional judgment and experience with common practice to make reasonable inferences of the patient's best interest in allowing a person to act on behalf of the individual.

SECTION 7 – PATIENT AUTHORIZATION FORM.

Except as stated in this Policy and consistent with the requirements of federal and state law, UAMS will not provide access to or disclose PHI without the patient’s Authorization. In addition, **UAMS will verify the identity of a person requesting PHI and the authority of the person to have access to PHI**, if the identity or authority of the person is not known to the personnel receiving the request for such information.

NOTE: Patient Directory. *If a person is asking for the information in the UAMS Patient Directory, the person only needs to identify the patient by name, and UAMS may release the location of the patient in our facility, and the patient’s general condition described in a one-word statement, such as good, fair, serious or critical, unless the patient has asked us not to. Please refer to UAMS Patient Directory Policy, 3.1.20.*

A. Requirements of Authorization: For an authorization from a patient or the patient’s Legal Representative to be valid, it must be written in plain language, and contain the following elements:

1. A specific description of the information to be used or disclosed.
2. The persons, or class of persons, authorized to make the requested use or disclosure.
3. The name (or other specific identification) of the persons, or class of persons, to whom UAMS may disclose the records.
4. A description of each purpose of the requested use or disclosure.
5. An expiration date or expiration event.
6. A statement that the person can revoke the authorization in writing, the process for revoking the authorization, and a statement that the person cannot revoke authorization for records already released in reliance upon the authorization.
7. A statement that UAMS will not condition treatment or payment on the whether the individual signs the authorization, **unless** the authorization is for research purposes, and then UAMS may condition research-related treatment upon the signing of the authorization.
8. A statement that records or information in the records released might be redisclosed by the person receiving them and will not be covered under the federal privacy laws.
9. Signature of the patient and date; and
10. If the authorization is signed by a Legal Representative of the patient, a description of the Representative’s authority to act for the patient, (e.g., “parent of a minor,” “Court-appointed guardian,” “health care proxy,” “pursuant to appointment under Power of Attorney.”)

B. UAMS Authorization Forms: The following forms are available and attached to this Policy:

1. UAMS Authorization for Release of Information From UAMS
2. UAMS Authorization for Release of Information To UAMS
3. UAMS Authorization for Release of Psychotherapy Notes
4. UAMS Substance Abuse Clinic Authorization for Release of Confidential Information
5. UAMS Office of Communications HIPAA Authorization to Allow Access to Patients

- C. Authorizations Requested by UAMS:** If UAMS requests a written authorization from the patient to release records, the authorization must contain those items in Paragraph A above.
- D. Combining Authorizations:** The authorization may not be combined with any other document except as follows:
1. A patient authorization for use and disclosures created for a research study may be combined with any other type of written permission for the same research study; or
 2. A patient authorization for a use or disclosure of Psychotherapy Notes may only be combined with another authorization for a use or disclosure of Psychotherapy Notes.
- E. Conditioning:** UAMS will not condition provision of treatment or payment on obtaining patient authorization to use or disclose PHI except under the following circumstances:
1. Research related treatment; or
 2. Provision of health care solely for the purpose of creating PHI for disclosure to a third party, for example pre-employment physicals.
- F. Continuing Effect of Authorization:** A valid authorization shall be effective for the release of PHI for 90 days from the date it is signed unless the authorization specifies a different period of time, or the patient or patient's Legal Representative later revokes the authorization.
- G. Patient's Revocation of Authorization:** The patient has the right to revoke/cancel his or her Authorization previously given to UAMS. The revocation must be in writing, signed by the patient, and delivered to the Medical Records Department of the appropriate UAMS clinic or to the UAMS Health Information Management office. The revocation will not apply to records already released in reliance upon the Authorization.
- H. Photocopies of Authorization:** A photographic copy or facsimile of a signed authorization may be accepted, as long as the authorization otherwise meets the requirements of this Policy.
- I. Provide Copy of Authorization to Patient/Patient's Representative:** When patient or patient's Legal Representative signs an Authorization for Release of Information Form, a copy of the signed form must be provided to the person signing the form.
- J. Authorization for Release of Decedent's Records:** An Authorization to release PHI of a deceased person can be signed by the following:
1. The parent of a deceased minor; or
 2. A person appointed by a court to act on behalf of the estate of the deceased, such as an Executor or Administrator. If the Authorization is signed by a person stating he or she has been appointed by a court to act on behalf of the estate of the deceased, a copy of the court order is required; or
 3. Other persons authorized by law to act on behalf of the deceased individual or the estate of the deceased individual.

(If the request for the release of the records is for the purpose of providing treatment to a surviving relative of the deceased individual, the records may be released to the relative's physician without an authorization.)

- K. Authorization for Unemancipated Minor:** Generally - An authorization for release of PHI concerning a minor (under 18 years of age) who is unemancipated (living at home, and dependent on parents for financial support, education, medical care, etc.) can only be given by a parent or legal guardian of the patient
- L. Authorization of Unemancipated Minor of Divorced or Separated Parents:** If the parents are divorced or legally separated, either parent (who has not had his/her parental rights terminated by the court) may sign the authorization unless a valid court order specifies otherwise.
- M. Authorization of Emancipated Minor:** An authorization for release of PHI concerning a minor (under 18 years of age) who is emancipated (not living at home and not dependent on parents for support, medical care, education, etc.) can only be given by the patient himself.
- N. Authorization by One Standing in Loco Parentis:** An authorization for release of PHI concerning a minor (under 18 years of age) who is unemancipated may be given by an adult who stands "in loco parentis" to the minor. (A person standing "in loco parentis" is one who is responsible for providing all support for the minor.)
- O. Keep Authorization in Record:** The original or a copy of every authorization to release PHI will be maintained as a permanent part of the medical record.
- P. Refusal to Honor Authorization:** UAMS may refuse to honor an authorization in the following situations:
 1. When there is a question as to the identity or authority of the person requesting release of the records;
 2. When there is a doubt that the person requesting the information is the person named in the authorization;
 3. If UAMS has knowledge that the person who signed is not of legal age or is incompetent;
 4. When there is a question as to the legal guardian of a minor or incompetent patient;
 5. When there is a reason to know the patient may not want the authorization honored;
 6. When there is any question as to the authenticity of the signature of the patient or person signing on behalf of the patient;
 7. When the requirements of this policy have not been met; or
 8. If there is a reasonable belief that a minor patient has been abused or neglected and that releasing the record to the personal representative requesting it might endanger the child.

SECTION 8 - DISCLOSURE OF INFORMATION OUTSIDE UAMS FOR PURPOSES UNRELATED TO TREATMENT, PAYMENT AND OPERATIONS.

- A. General Rule Concerning Disclosure Outside UAMS:** UAMS may not release PHI externally unless it is in accordance with UAMS policies and consistent with federal, state and local laws, rules and regulations.
- B. Verification:** UAMS will verify the identity and authority of the person requesting PHI.
- C. Disclosure of Information to Attorneys:** PHI shall not be released to any attorney (including an attorney of the patient) unless the request is accompanied by a proper Authorization from the patient (or patient's Legal Representative authorized by law to act on behalf of the patient concerning health care matters), and the authorization must contain the required elements of an Authorization stated above. The request must meet all other applicable requirements of this policy. If the attorney is requesting the records for a family member or any other person claiming to have the authority to act on behalf of the patient, the authority of the person to act on behalf of the patient must be verified in accordance with this Policy.
- D. Disclosure of Information to the News Media:** All requests for releases of PHI to the news media should be referred to the UAMS Office of Communications and Marketing.

- E. **Disclosure of Information to Patient's Employer:** PHI shall not be released directly to a patient's employer unless the request is accompanied by a proper Authorization from the patient, and the request meets the applicable requirements of this Policy. If you are providing PHI directly to the patient for the patient to provide to an employer, then the Authorization Form is not required.
- F. **Disclosure of Information to Schools:** PHI shall not be released to school personnel, teachers, or school nurses unless the request is accompanied by a proper Authorization as required by this Policy, and the request meets the applicable requirements of this Policy. If you are providing PHI directly to the patient for the patient to provide to a school, then the Authorization Form is not required.
- G. **Disclosure of Psychotherapy Notes:** Psychotherapy notes are separate from and are not a part of a patient's medical record or contained in a Designated Record Set. The use and disclosure of psychotherapy notes is very limited. Psychotherapy notes may be used only by the originator of the notes to carry out treatment, or by UAMS for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family or individual counseling; or for UAMS to defend itself in a legal action or other proceeding brought by the patient, or by health learn under supervision to practice or improve their skills in counseling, or by UAMS as required by law. All other uses or disclosures of psychotherapy notes require the patient's authorization using a separate authorization form. An example of an Authorization for Release of Psychotherapy Notes is attached to this Policy. See definition of "Psychotherapy Notes" stated in this Policy and refer to UAMS [Psychotherapy Notes Policy, 3.1.24](#) for additional information.
- H. **Adoption Records:** Adoption information and records shall be confidential and shall not be released without a court order authorizing release to a specific person. Any questions pertaining to release of adoption records should be referred to Office of General Counsel.

SECTION 9 – REQUIRED BY LAW – No Patient Authorization Required.

UAMS may use or disclose PHI to the extent required by law, with the condition that:

(a) the PHI used or disclosed is limited to the relevant requirements of such law; and (b) the disclosure is made only to the authorities authorized to receive the information.

"Required by law" generally means a requirement in the law that compels an entity to make a use or disclosure of information that is enforceable in a court of law. For example, some state and federal statutes or regulations require hospitals to report certain health information to the Arkansas Department of Health, the Arkansas Department of Human Services, the Arkansas State Medical Board, the Arkansas State Board of Nursing, or the Arkansas Pharmacy Board.

The following list of reporting requirements stated below is not intended to be all inclusive, but merely to show examples.

- A. **Births and Deaths:** Arkansas Department of Health, Division of Vital Records, must receive reports of births and deaths occurring at UAMS, pursuant to Ark. Code Ann. § 20-18-401 and Ark. Code Ann. § 20-18-601, respectively.
- B. **Deaths from Suspicious Circumstances, Criminal Conduct or Other:** UAMS must notify the county coroner and the chief law enforcement official of the county and town/city in which a death occurred if UAMS has knowledge of the death, and UAMS suspects that the death occurred as a result of violence, criminal conduct or of any of the other circumstances listed in Ark. Code Ann. § 12-12-315. Also see Section 13 of this Policy for partial list.

- C. **Disease and Disease Prevention:** Arkansas Department of Health must receive reports of a positive test at UAMS for the presence of conditions or diseases identified by statute such as the reporting of sickle cell anemia, and any case or suspected case of Reye's Syndrome. Immunizations given to persons under 22 years old must be reported to the Arkansas Department of Health. Ark. Code Ann. §§ 20-15-302, 20-15-401, 20-15-1203.
- D. **Sudden Infant Death Syndrome:** The County Coroner must receive reports of the sudden death of a child between the ages of one (1) week and one (1) year who appeared in apparent good health, as required by Ark. Code Ann. § 20-15-502. If the County Coroner is unavailable, the report is made to the County Sheriff. The County Coroner or County Sheriff reports the death to the Arkansas Department of Health.
- E. **Child Maltreatment/Abuse/Neglect:** The DHS Arkansas Child Abuse Hotline must receive reports if any health care professional or medical personnel at UAMS has reasonable cause to suspect that a child under 18 years of age has been subjected to maltreatment, abuse, neglect, sexual exploitation or abandonment; and the Arkansas Department of Human Services and Law Enforcement Officials shall have access to medical records, photographs or videotapes relating to the existence or extent of the maltreatment, abuse or neglect. Ark. Code Ann § 12-12-506 through § 12-12-508.
- F. **Abuse of Elderly, Endangered or Impaired Adult:** The Arkansas Department of Human Services (including the Office of Long Term Care), the Office of Attorney General, the County Prosecutor, the County Coroner, and the Adult Abuse Hotline are entitled to receive information if any health care professional or employee of UAMS has reasonable cause to suspect the abuse or neglect of an endangered or impaired adult or an adult residing in a long-term care facility and shall have access to the medical records or other information requested in connection with the investigation of suspected abuse or neglect. Ark. Code Ann. § 5-28-203, § 5-28-204, and § 5-28-209.
- G. **Intentional Infliction of Knife or Gunshot Wounds:** The Office of the County Sheriff and the City Police are entitled to receive information in connection with all cases of knife or gunshot wounds treated by UAMS or while in UAMS, if the wounds appear to have been intentionally inflicted. Ark. Code Ann. § 12-12-602.
- H. **Venereal Disease:** The Division of Health Maintenance of the Arkansas Department of Health must be notified when a laboratory examination determines that a specimen from a human body yields microscopic, cultural, serological, or other evidence suggestive of a venereal disease. Ark. Code Ann. § 20-16-501.
- I. **HIV:** The Arkansas Department of Health must receive reports of any person determined to have AIDS or to have tested positive for HIV. Ark. Code Ann. § 20-15-905 and 20-15-906.
- J. **U.S. Department of Health and Human Services:** UAMS must disclose PHI to the Secretary of the U.S. Department of Health and Human Services for purposes of investigating or determining UAMS' compliance with HIPAA regulations.
- K. **State Cancer Registry:** UAMS must disclose certain PHI concerning incidents of cancer to the Arkansas Department of Health's State Cancer Registry. Ark. Code Ann. § 20-15-201.

The identity and authority of the person to whom the patient's PHI is being disclosed must be verified, if not known, prior to the disclosure.

NOTE: For all such disclosures under this Section, see UAMS [Accounting for Disclosures Policy, 3.1.26](#).

SECTION 10 – REPORTING TO AGENCIES or OTHERS AUTHORIZED BY LAW TO RECEIVE THE INFORMATION – No Patient Authorization Required, But Certain Limitations.

UAMS may use or disclose PHI, without patient authorization, when required or allowed to do so by law for the purpose of reporting to governmental agencies or other authorized individuals, with the condition that (a) the PHI

disclosed is limited to the relevant requirements of such law; (b) the disclosure is made only to the authorities authorized to receive the information; and (c) the PHI disclosed is limited to the minimum necessary required for the intended use or purpose of the information. The release of PHI under these circumstances does not change the requirement to protect and maintain the confidentiality of the patient's PHI.

The identity and authority of the person to whom the patient's PHI is being disclosed must be verified. UAMS [Verification of Identity Policy, 3.1.37](#).

- A. Public Health Authorities:** UAMS may disclose PHI to public health authorities authorized by law to receive such information when the disclosure is made in connection with a public health concern, such as for the purpose of preventing or controlling disease, injury, or disability, for the purpose of reporting to the FDA, or to notify persons who may have been exposed to a communicable disease if authorized under state law to do so.
- B. Health Oversight Agencies:** Health oversight agencies are agencies of the state or federal government, or entities acting under a grant of authority or contract with the public agency, which are authorized by law to oversee the health care system or government programs in which health information is necessary to determine eligibility or compliance. UAMS may disclose PHI to health oversight agencies for health oversight purposes authorized by law, including audits, investigations, inspections, licensure or disciplinary actions, and other activities necessary for appropriate oversight of the health care system. For example, Medicare and Medicaid, State licensure boards, DHHS Office of Inspector General, and DHHS Office for Human Research Protections or other agencies authorized by law to oversee the health care system.
- C. Coroners and Medical Examiners:** UAMS may disclose PHI to coroners and medical examiners for the purpose of identifying a deceased person, for determining a cause of death, or for coroner or medical examiner to perform other duties authorized by law.
- D. Funeral Directors:** UAMS may disclose PHI as needed for the funeral director to carry out their duties. UAMS may share PHI prior to, and in reasonable anticipation of, the patient's death.
- E. Organ/Eye/Tissue Donation Organizations:** UAMS may use or disclose PHI to an organ procurement organization or entity engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.
- F. Workers' Compensation:** UAMS may disclose PHI to comply with the laws relating to workers' compensation or other similar programs that provide benefits for work-related injuries or illness without regard to fault.

NOTE: For all such disclosures under this Section, see UAMS [Accounting for Disclosures Policy, 3.1.26](#).

SECTION 11 - COURT ORDERS, WARRANTS AND GRAND JURY SUBPOENAS – No Patient Authorization Required.

UAMS may disclose PHI, without patient authorization, as directed by the following:

1. a court order;
2. a court-ordered warrant; or
3. a grand jury subpoena.

The PHI disclosed must be limited to the PHI described in and required by the order, warrant or grand jury subpoena.

In addition, the PHI must be disclosed only to those persons identified in the order, warrant or grand jury subpoena as

persons directed to receive the information.

NOTE: For all such disclosures under this Section, see UAMS [Accounting for Disclosures Policy, 3.1.26](#).

SECTION 12 – SUBPOENAS and DISCOVERY REQUESTS FROM PARTIES IN LITIGATION – Patient Authorization, Court Order, or Written Assurances Required.

A. General. This Section covers subpoenas and discovery requests from parties in litigation: This Section does not cover subpoenas from a Grand Jury or from Law Enforcement. UAMS may disclose PHI in response to a valid subpoena or in response to a discovery request by parties in litigation only if UAMS also receives any one of the following:

1. An Authorization signed by the patient or patient’s Legal Representative.
 - a. The Authorization must authorize release of the records described in the subpoena or include a description broad enough to encompass the records described in the subpoena.
 - b. The Authorization must authorize release of the records to the person or persons identified in the subpoena.
 - c. The Authorization must be a HIPAA compliant Authorization containing the elements described in this Policy.
 - d. A patient’s attorney is not the patient’s “Legal Representative” for purposes of signing an Authorization. If the Authorization is not signed by the patient, it must be signed by the patient’s “Legal Representative” who is a person authorized by law to act on behalf of the patient. For example, a court-appointed guardian, a person designated as the patient’s attorney-in-fact in a power of attorney, or the parent of an unemancipated minor.
2. A court order, or an order of an administrative tribunal such as the Workers’ Compensation Commission.
3. Written assurances that patient was notified of the subpoena for the patient’s records, and the patient does not object to the production of the records, or the patient’s objections were overruled by the court. To provide such written assurances, the party seeking the patient’s records by subpoena must submit a written statement and documentation to UAMS showing that:
 - a. reasonable efforts have been made by such party to ensure that the patient has been notified of the subpoena for the patient’s records;
 - b. the notice to the patient included sufficient information about the litigation or proceeding to permit the patient or patient’s attorney to file objections with the court or administrative tribunal;
 - c. the time for filing objections has elapsed; and
 - d. no objections were filed, or if objections were filed, the court or administrative tribunal ordered the disclosure, and a copy of the order should be provided.

These written assurances may occur in stages. For example, UAMS may first receive the subpoena, along with documentation showing that a copy of the subpoena was provided to the patient or the patient’s attorney. After the time for filing objections has passed, UAMS may later receive the written assurance that the time for filing objections has passed and the patient did not object.

B. Subpoena Without Authorization, Court Order, or Written Assurances: If a subpoena for patient’s PHI does not include any other authority for releasing the records, such as the patient’s Authorization, a court order,

or the written assurances described above, UAMS is not authorized to release the records. UAMS should undertake reasonable efforts to inform the party seeking the records, prior to the date of production stated in the subpoena if possible, that

UAMS is not authorized to release the records without the required Authorization, court order, or written assurances.

NOTE: If no signed patient Authorization (HIPAA-compliant) and for all such disclosures under this Section, see UAMS [Accounting for Disclosures Policy, 3.1.26](#).

SECTION 13 – SUBPOENAS FROM LAW ENFORCEMENT OFFICIALS.

No Patient Authorization Required, But Certain Limitations.

- A. General:** UAMS may disclose PHI to law enforcement officials in response to a valid subpoena, Investigative Demand (which is usually headed “Investigative Demand”), or similar process authorized by law, as long as:
- (a)** The information requested is relevant and material to a legitimate law enforcement inquiry;
 - (b)** The request is specific and limited in scope to the extent reasonably practicable in light of the purpose from which the information is sought; and
 - (c)** de-identified information could not reasonably be used.
- B. Law Enforcement Official:** Law Enforcement Official means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to: (1) Investigate or conduct an official inquiry into a potential violation of law; or (2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

This would include subpoenas from the Arkansas Office of Attorney General, the Prosecuting Attorney’s Office, the FBI, and the police.

NOTE: For all such disclosures under this Section, see UAMS [Accounting for Disclosures Policy, 3.1.26](#).

SECTION 14 – LAW ENFORCEMENT GENERALLY (Without Court Order or Warrant, Subpoena, or Other Legal Process) – No Patient Authorization Required, But Certain Limitations.

A. Disclosures for Identification and Location of Suspect, Fugitive, Material Witness or Missing Person:

- 1. PHI Allowed to be Disclosed:** In response to law enforcement’s request or notice for information to identify or locate a suspect, fugitive, material witness or missing person, UAMS may disclose the following information only:
 - a. name and address;
 - b. date and place of birth;
 - c. Social Security Number;
 - d. ABO blood type and rh factor;
 - e. type of injury;
 - f. date and time of treatment;
 - g. date and time of death, if applicable; and
 - h. description of distinguishing physical characteristics, such as weight, height, gender, race,

hair/eye color, presence or absence of facial hair, scars, tattoos.

2. **Disclosure Not Allowed:** UAMS may not disclose the following information in response to law enforcement's request or notice for information to identify or locate a suspect, fugitive, material witness or missing person:
 - a. DNA or DNA analysis;
 - b. dental records;
 - c. typing, samples or analysis of body fluids or tissue.

B. To Prevent or Lessen Serious and Imminent Threat to Health or Safety:

1. **Disclosures to Law Enforcement:** UAMS may, consistent with the law and standards of ethical conduct, use or disclose PHI to a Law Enforcement Official, without patient authorization or other authority, if UAMS believes in good faith that the use or disclosure is:
 - a. necessary to prevent or lessen a serious and imminent threat to the health or safety of any person or the public;
 - b. and the disclosure is (i) to persons reasonably able to prevent or lessen the threat, such as law enforcement; or (ii) the disclosure is necessary for law enforcement to identify or apprehend an individual because of a statement made by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim or where it appears from the circumstances that the individual has escaped from a correction institution or from lawful custody.
2. **Disclosures to Others:** UAMS may, consistent with the law and standards of ethical conduct, use or disclose PHI, without patient authorization or other authority, if UAMS believes in good faith that the use or disclosure is:
 - a. necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public;
 - b. and the disclosure is (i) to persons reasonably able to prevent or lessen the threat, including the target of the threat; or (ii) the disclosure is necessary for law enforcement to identify or apprehend an individual because of a statement made by an individual admitting participation in a violent crime that the covered entity reasonably believes may have caused serious physical harm to the victim or where it appears from the circumstances that the individual has escaped from a correctional institution or from lawful custody.

C. To Report a Crime on UAMS Property: UAMS may disclose PHI to a Law Enforcement Official if UAMS believes in good faith that the PHI disclosed constitutes evidence of criminal conduct that occurred on the premises of UAMS.

D. Deaths: UAMS must notify the county coroner, the chief law enforcement official of the county, and the chief law enforcement official of the town/city where the death occurred if UAMS has knowledge of the death and any of the following circumstances appear to exist:

1. death was caused by violence, homicide, suicide or appears to be accidental;
2. death resulted from presence of drugs or poisons in the body;
3. death resulted from drowning;

4. death resulted from motor vehicle accident or body was found in or near a roadway or railroad;
5. death occurred in hospital and no previous medical history to explain the death;
5. death occurred while person in policy custody, a jail, or penal institution;
7. death resulted from fire or explosion;
3. death of minor indicated child abuse prior to death;
9. death of minor and no prior medical history to explain the death;
10. human skeletal remains were recovered or unidentified deceased person was discovered;
11. death was due to criminal abortion;
12. manner of death was from other than natural causes;
13. death was sudden and unexplained;
14. death occurred at work site; or
15. death occurred in the home.

See Arkansas Code Ann. 12-12-315 for additional examples.

- E. Suspected Child Abuse or Neglect:** If there is reasonable cause to suspect that a child has been subjected to abuse/neglect or has died as a result of abuse/neglect, or if a child is observed being subjected to conditions or circumstances that would reasonably result in child abuse/neglect, UAMS must use and disclose PHI for purposes of contacting the Arkansas Child Abuse Hotline and reporting to the authorities authorized by law to receive such information, such as the Arkansas Department of Human Services and other Law Enforcement Officials investigating the suspected abuse/neglect.
- F. Abuse of Elderly, Endangered or Impaired Adult:** UAMS must use and disclose PHI to the Arkansas Department of Human Services (including the Office of Long Term Care), the Office of Attorney General, the County Prosecutor, the County Coroner, or the Adult Abuse Hotline if UAMS has reasonable cause to suspect the abuse or neglect of an endangered or impaired adult or an adult residing in a long-term care facility and these agencies may have access to the medical records or other information requested in connection with the investigation of suspected abuse or neglect.
1. **Informing the victim is required:** If UAMS makes a disclosure in the case of abuse of elderly, endangered or impaired adults, UAMS must promptly inform the patient/victim that such a report has been or will be made. See exceptions below.
 2. **You do not have to inform the victim in certain limited circumstances:** Informing the patient/victim that UAMS has or will report the suspected abuse/domestic violence is not required **if:** (1) UAMS believes, in the exercise of professional judgment, that informing the individual would place the individual at risk of serious harm; or (2) UAMS would be informing a Legal Representative of the

patient who is authorized by law to act on behalf of the patient (such as a court-appointed guardian), and UAMS reasonably believes the Legal Representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the patient/victim.

G. Other Law Enforcement Purposes: PHI also may be used and disclosed without patient authorization or permission in the following circumstances:

1. For specialized government activities including military and veterans' activities, national security and intelligence activities and protective services for the President and others.
2. To correctional institutions and law enforcement officials about an individual who is an inmate or is in their lawful custody if necessary for the health and safety of the individual, other inmates, officers or other employees at the correctional institution, or persons responsible for the inmate's transportation or otherwise for the administration and maintenance of the safety, security and good order of the correctional institution
3. If emergency medical care is provided, other than on the premises of UAMS, and disclosure of PHI appears necessary to alert law enforcement to: (a) the commission and nature of a crime; (b) the location of the crime or the victims of the crime; or (c) the identity, description and location of the perpetrator of the crime.

NOTE: For all such disclosures under this Section, see UAMS [Accounting for Disclosures Policy, 3.1.26](#).

SECTION 15 – ADULT VICTIMS OF ABUSE, NEGLECT or DOMESTIC VIOLENCE – Reporting to Authorities Requires Patient Consent.

- A. Victim's Consent Required:** *Except for* the circumstances listed below in "Exceptions," UAMS must obtain the written or verbal consent of a patient (age 18 or older) whom UAMS reasonably believes to be a victim of abuse or domestic violence *before* UAMS can report the suspected abuse or domestic violence to a government authority authorized by law to receive such reports, such as the police, DHS, a social services agency or a protective services agency. (If the government authority authorized by law to receive such reports presents a subpoena, court order or warrant, then refer to the various Sections in this policy regarding subpoenas, court orders and warrants, whichever is applicable.)

The consent may be written or verbal: An Authorization form is not required, but may be used. Once consent is given, the medical evidence relevant to the victim's injuries and the alleged crime may be disclosed.

- B. Exceptions:** Victim consent is not required for:

1. Reports of abuse/neglect of a child under 18.
2. Reports of abuse/neglect of the elderly or an impaired or endangered adult.
3. Disclosures of certain limited information to Law Enforcement to identify or locate a suspect, fugitive, material witness or missing person. See section of this Policy entitled "Law Enforcement Generally."
4. All other disclosures required by law and to the extent that the disclosure complies with and is limited to the relevant requirements of such law (such as reporting deaths, intentional inflicting of gunshot or knife wounds, and other reporting requirements). See section of this Policy entitled "Law Enforcement Generally" and see "Required by Law" section for disclosures required by law.
5. Disclosures made pursuant to a court order, warrant or other similar legal process enforceable in a court or law.

- C. If Victim Incapacitated:** If UAMS is unable to obtain the victim's agreement because the victim is incapacitated, UAMS can disclose the victim's PHI only if all of the elements of "Circumstances ONE" or "Circumstances TWO" exist:

Circumstances ONE

1. The disclosure is expressly permitted by statute or regulation; and
2. The Law Enforcement Official represents that (a) such information is needed to determine whether a violation of law by a person *other than* the victim has occurred, and (b) such information is not intended to be used against the victim; and
3. The Law Enforcement Official represents that immediate law enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

OR

Circumstances TWO:

1. The disclosure is expressly permitted by statute or regulation; and
2. UAMS workforce members involved believe that, in the exercise of professional judgment, the disclosure is necessary to prevent serious harm to the individual or other potential victims.

D. When Informing the Victim of Disclosure/Report is Required:

1. **Informing the victim is required:** If UAMS makes a disclosure with the consent of the patient/victim, as described above, or in the case of abuse of elderly, endangered or impaired adults where consent is not required, UAMS must promptly inform the patient/victim that such a report has been or will be made. See exceptions below.
2. **You do *not* have to inform the victim in certain limited circumstances:** Informing the patient/victim that UAMS has or will report the suspected abuse/domestic violence is not required **if:** (1) UAMS believes, in the exercise of professional judgment, that informing the individual would place the individual at risk of serious harm; or (2) UAMS would be informing a Legal Representative of the patient who is authorized by law to act on behalf of the patient (such as a court-appointed guardian), and UAMS reasonably believes the Legal Representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the patient/victim.

NOTE: If no signed patient Authorization (HIPAA-compliant) and for all such disclosures under this Section, see UAMS [Accounting for Disclosures Policy, 3.1.26](#).

SECTION 16 -- ADULT VICTIMS OF RAPE, ATTEMPTED RAPE, SEXUAL ASSAULT OR INCEST -- Reporting to Authorities Requires Patient Consent.

UAMS will follow the requirements of Arkansas law, Ark. Code Ann. 12-12-401 through 12-12-405 regarding treatment of victims of rape, attempted rape, sexual assault or incest.

If an adult patient, age 18 years or older, is presented for treatment as a victim of rape, attempted rape, any other type of sexual assault, or incest, the adult patient shall make the decision of whether the incident will be reported to a law

enforcement agency. If consent is given to UAMS to contact law enforcement on behalf of the victim, the consent may be given verbally. A HIPAA-compliant authorization is not required, but may be used.

UAMS may not require an adult victim to report the incident in order to receive medical treatment. Evidence will be collected only with the permission of the victim. However, permission to collect such evidence shall not be required in instances where the victim is unconscious, mentally incapable of consent or intoxicated. Once evidence is collected, it will be provided to law enforcement with the permission of the victim.

See UAMS [Policy ML.1.08](#) regarding sexual assault of adult.

NOTE: If no signed patient Authorization (HIPAA-compliant) and for all such disclosures under this Section, see UAMS [Accounting for Disclosures Policy, 3.1.26](#).

SECTION 17 – SUBSTANCE ABUSE/TREATMENT INFORMATION – Patient Authorization Requiring Using Substance Abuse Treatment Form.

- A. Patient Authorization Required:** For patients of the UAMS Substance Abuse Treatment Center or any other UAMS substance abuse treatment program, the patient’s signed Authorization must be obtained before UAMS can disclose any PHI relating to the diagnosis, prognosis, treatment, or referral for treatment in relation to substance abuse (drug or alcohol), including any information which would identify the person as being a patient in such a program, or acknowledgment or confirmation that the person is or was a patient in such a program.

Access the UAMS [Substance Abuse Treatment Authorization](#) form.

- B. Exceptions:** An authorization signed by the patient is not required in very limited circumstances, such as pursuant to a court order directing the disclosure of information or records specifically relating to substance abuse. Consult the UA Office of General Counsel for further information in response to a request or subpoena for such information in the absence of a court order or patient Authorization.

SECTION 18. MINORS.

- A. Release of Minors’ PHI to Minors’ Parents:** Generally, the parent of a dependent child under the age of 18 is entitled to all PHI concerning their minor child, regardless of whether the parents are divorced. A divorced parent who does not have custody of the minor child is still the minor’s parent, and is entitled to all PHI concerning their minor child. **See exceptions below.**
- B. Release of Minors’ PHI to Minors’ “Legal Representative:”** The “Legal Representative” of a child is one who has legal authority to act on behalf of the child, including the authority to make health care decisions for the child. Examples are (1) the parent; (2) a court-appointed Guardian; (3) a person legally acting as a parent (“*in loco parentis*” – the person has physical custody and supervision of the child, and the child lives with and is supported by the person); or (4) any other court order providing the person with legal custody or the legal authority to act on behalf of the child.
- C. Exceptions to Providing PHI to Parent or Legal Representative of Minor Child:** UAMS is not required to provide a person who has authority to act on behalf of a minor with the PHI of the minor in the following circumstances:
1. **Court Order:** A court order terminates the parental rights of the parent over the minor child or children. Issues relating to custody do not apply. The court order must specifically terminate the parent’s rights.
 2. **Not in Best Interest of Child:** UAMS has a reasonable belief that the child has been or may be subjected to domestic violence, abuse or neglect by such person, *or* if UAMS has a reasonable belief that

the person may cause physical or emotional harm to the child, *or* if UAMS determines in the exercise of professional judgment that it is not in the best interest of the child to release the information.

3. **Biological Father of Child Born Out of Wedlock:** The request for information is by the biological father of a child born out of wedlock, who does not have physical custody of the child, and who is not married to the mother at the time of the request. The biological father must provide a copy of a court order providing the father with legal custody, parental rights or some other authority to act on behalf of the child or to receive information.
4. **Venereal Disease:** The minor has consented to their own treatment for a known or suspected venereal disease. However, the treating physician *may* release the information to the minors' parents or Legal Representatives if the treating physician determines that the information should be released, even over the objections of the minor. This does not prohibit the confidential reporting of a confirmed case of a venereal disease to the Arkansas Department of Health as required under Arkansas law. All records of such information concerning the minor's known or suspected venereal disease should be maintained in a manner that the user can determine immediately and easily that the records are confidential and are not to be released with the rest of the medical record.

SECTION 19. EMERGENCY CIRCUMSTANCES – No Patient Authorization Required.

NOTE: For purposes of this Section, when “**good faith**” is required, “good faith” is presumed to exist if it is based upon the actual knowledge of UAMS or is based upon UAMS' reliance on a credible representation by a person with apparent knowledge or authority.

- A. **To Prevent or Lessen Serious and Imminent Threat to Health or Safety:** UAMS may, consistent with the law and standards of ethical conduct, use or disclose PHI if UAMS believes in good faith that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of any person or the public in general; and the disclosure is to persons reasonably able to prevent or lessen the threat, such as to law enforcement or to the target of the threat or to others reasonably able to prevent or lessen the threat.
- B. **Admission by Patient of Participation in Violent Crime:** UAMS may, consistent with the law and standards of ethical conduct, use or disclose certain PHI to law enforcement authorities if UAMS believes in good faith that the use or disclosure is necessary for law enforcement authorities to identify or apprehend an individual because of a statement made by an individual admitting participation in a violent crime that UAMS reasonably believes may have caused serious physical harm to the victim. (See “Exceptions” listed below.)
 1. **Limited PHI to be Used/Disclosed:** In such circumstances where there has been an admission by a patient as described above, UAMS may disclose to law enforcement authorities the following information concerning the patient:
 - a. name and address;
 - b. date and place of birth;
 - c. Social Security Number;
 - d. ABO blood type and rh factor;
 - e. type of injury;
 - f. date and time of treatment;

- g. date and time of death, if applicable; and
- h. description of distinguishing physical characteristics, such as weight, height, gender, race, hair/eye color, presence or absence of facial hair, scars, tattoo.

DNA or DNA analysis, dental records, typing, samples or analysis of body fluids or tissue, or any other PHI may not be disclosed without a court order or warrant or other legal process.

- 2. **Exceptions -- Use/Disclosure Prohibited:** Such a use or disclosure may not be made if the admission of the patient is learned by UAMS (1) in the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the disclosure, (2) in counseling of therapy of the patient; or (3) through a request by the patient to initiate or to be referred for the treatment, counseling, or therapy to affect the propensity to commit the criminal conduct that is the basis for the disclosure.
- C. **To Identify or Apprehend Escaped Prisoner:** UAMS may, consistent with the law and standards of ethical conduct, use or disclose PHI to law enforcement authorities if UAMS believes in good faith that the use or disclosure is necessary for law enforcement authorities to identify or apprehend an individual where it appears from the circumstances that the individual has escaped from a correctional institution or from lawful custody.
- D. **Medical Emergencies:** UAMS may disclose PHI to a person who is the spouse, family or friend involved in the patient's care, without patient's consent or Authorization, in the event of a medical emergency.

SECTION 20 – PATIENT REQUEST TO AMEND RECORD.

A patient has the right to request UAMS to amend his or her PHI maintained in the Designated Record Set. UAMS is not required to agree to all requests by patients to amend their records. Requests to amend will be referred to the Release of Information Office in Health Information Management/Medical Records Department and processed in accordance with the UAMS [*Patient Request to Amend the Medical Record Policy, 3.1.32.*](#)

SECTION 21- COSTS OF OBTAINING COPIES OF MEDICAL RECORDS.

UAMS may charge a reasonable, cost-based fee for copies of medical records that includes the cost of copying, cost of supplies and labor of copying, and postage, when the patient has requested the copy be mailed. UAMS will not charge more than is allowed by law and pursuant to Ark. Code Ann. § 16-46-106.

SECTION 22 – SANCTIONS/DISCIPLINARY ACTION.

UAMS workforce who engage in activity in violation of this Policy may be subject to disciplinary action, up to and including termination of employment or relationship with UAMS.

Place Patient Label Here or

Print Patient Name

Authorization for Release of Information from UAMS

1. I, _____, hereby authorize UAMS to release to:

Name _____ Phone _____ Fax _____

Address _____
Street Address City State Zip

2. Information of:

Patient Name _____ Medical Record No. (if known) _____

Date of Birth and/or Social Security No. _____ Phone _____

3. Information is to be limited to the following **Dates of Treatment** (if applicable): _____

4. Information requested to be accessed or released:

____ Abstract ____ Operative Report ____ ER Record ____ History & Physical ____ Discharge Summary
 ____ Clinic Record ____ Admission Record ____ Physicians' Progress Notes ____ Nurses' Progress Notes
 ____ Other _____

____ Records of Other Providers on File With UAMS (if any) *(We must impose our standard copying fees as stated below. UAMS does not represent that these records are the complete records of the other providers. If you want a complete copy of the records created by the other providers for this patient, you may wish to contact each provider.)*

I understand that **if** the records requested to be released include information relating to **sexually transmitted disease, AIDS or HIV, alcohol or drug abuse, or mental health information**, this information may be released pursuant to this authorization.

5. ____ Billing Records. For hospital billing records, please contact Patient Business Services (PBS) at (501) 614-2888. For physician billing records, please contact Medical College Physician's Group (MCPG) at (501) 614-2160, or 1-800-559-6274.

6. Purpose of access or release: ____ Medical Care ____ Insurance or Other Payment ____ At Request of the Patient
 ____ Other (explain): _____

7. This authorization will expire 90 days from the date on which it was signed unless I specify a different time period. Expiration Date or Event: _____. I understand that I may revoke this authorization at any time by giving written notice to UAMS. A revocation of this authorization will not apply to records already released in reliance upon the authorization. A photocopy of this signed authorization shall constitute a valid authorization.

8. UAMS, its employees and attending physicians are released from legal responsibility or liability for the release of the above information to the extent indicated and authorized herein.

9. I understand that once the above information is disclosed, it may be re-disclosed by the designated recipient and the information may no longer be protected by Federal privacy laws and regulations.

10. I agree to pay the copying cost, including other expenses allowed by law, such as the cost of any supplies, labor of copying, postage, or other expenses incurred by UAMS to provide the copies requested.

11. UAMS will not condition treatment, payment, enrollment or eligibility for benefits on your signing of this authorization.

Signature of Patient or Legal Representative _____ Date: _____

If Legal Representative, authority of Legal Representative _____

(such as parent of a minor, court-appointed guardian, administrator of estate of deceased, attorney-in-fact appointed with power of attorney, or health care proxy)

EPF Barcode
(3/04)

HIPAA **PROVIDE COPY TO PATIENT/LEGAL REPRESENTATIVE**

Place Patient Label Here **or**
 Print Patient Name

Authorization for Release of Information TO UAMS

1. I, _____, hereby authorize:

Name/Facility _____ Address _____

Street Address

City

State

Zip

Phone _____

Fax _____

2. To release to: UAMS Medical Center
 Dr./Clinic _____
 4301 West Markham, Mail # _____
 Little Rock, AR 72205
 Phone (501) _____
 Fax (501) _____

3. Information of:

Patient Name: _____

Medical Record No. (if known)

Date of Birth and/or Social Security No. _____ Phone: _____

4. Information is to be limited to the following **Dates of Treatment** (if applicable): _____

5. Information requested to be released:

_____ Abstract _____ Operative Report _____ ER Record _____ History & Physical _____ Discharge Summary
 _____ Clinic Record _____ Admission Record _____ Physicians' Progress Notes _____ Nurses' Progress Notes Other

6. Purpose of release: _____ Medical Care _____ Insurance or Other Payment _____ At the Request of the Patient
 _____ Other (explain): _____

7. This authorization will expire 90 days from the date on which it was signed unless I specify a different time period. Expiration Date or Event: _____. I understand that I may revoke this authorization at any time by giving written notice. A revocation of this authorization will not apply to records already released in reliance upon the authorization. A photocopy of this signed authorization shall constitute a valid authorization.

8. I understand that once the above information is disclosed, it may be re-disclosed by the designated recipient and the information may no longer be protected by Federal privacy laws and regulations.

9. Treatment, payment, enrollment or eligibility for benefits will not be conditioned on your signing this authorization.

Signature of Patient or Legal Representative _____ Date: _____

If Legal Representative, authority of Legal Representative _____
 (such as parent of a minor, court-appointed guardian, administrator of estate of deceased, attorney-in-fact appointed with power of attorney, or health care proxy)

Patient Label Here or



Authorization for Release of Psychotherapy Notes

I, _____, hereby authorize UAMS to release to:

Name _____ Phone: _____

Address: _____

Information of:

Patient Name _____ Medical Record No. (if known) _____

Date of Birth and/or Social Security No. _____ Phone: _____

Information is to be limited to the following Dates of Treatment (if applicable): _____

Information requested to be released: _____ Psychotherapy Notes Only.

I understand that if the records requested to be released include information relating to sexually transmitted disease, AIDS or HIV, alcohol or drug use, or mental health information, this information may be released pursuant to this authorization.

Purpose of access or release: _____ Medical Care _____ Insurance or Other Payment _____ At Request of the Patient
_____ Other (explain): _____

This authorization will expire on the following date: _____. If no date is specified, this authorization shall expire one (1) year from the date signed below. I understand that I may revoke this authorization at any time by giving written notice to UAMS except that a revocation of this authorization will not apply to records already released in reliance upon the authorization. A photocopy of the signed authorization shall constitute a valid authorization.

UAMS, its employees and attending physicians are released from legal responsibility or liability for the release of the above information to the extent indicated and authorized herein.

I understand that once the above information is disclosed, it may be re-disclosed by the designated recipient and the information may no longer be protected by Federal privacy laws and regulations.

I agree to pay the copying cost, including other expenses allowed by law, such as the cost of any supplies, labor of copying, postage, or other expenses incurred by UAMS to provide the copies requested.

UAMS will not condition treatment, payment, enrollment or eligibility for benefits on your signing of this authorization.

Name of Patient or Legal Representative _____ Date: _____

Legal Representative, authority of Legal Representative _____

(such as parent of a minor, court-appointed guardian, administrator of estate of deceased, attorney-in-fact appointed with power of attorney, or health care proxy)

Approved by Originator of Psychotherapy Note or other UAMS Mental Health professional:

Name _____ Signature: _____

HIPAA **PROVIDE COPY TO PATIENT/LEGAL REPRESENTATIVE**

Date: _____ Signature of Witness

If signed by Legal Representative on behalf of patient, state authority of Legal Representative, such as parent, court-appointed guardian, health care proxy, appointed by patient in Power of Attorney document or other: _____

* 42 CFR Part 2 Statement is to be sent with each release of information: _____ Yes _____ No

(If NO explain) _____

Provide Patient With Copy of This Authorization After Patient Signs

17-A-0603

This information has been disclosed to you from records protected by Federal confidentiality rules (42 CFR Part 2). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient.



Place Patient Label Here

Print Patient Name

UAMS OFFICE OF COMMUNICATIONS

**HIPAA AUTHORIZATION TO ALLOW ACCESS TO PATIENTS
AND TO RELEASE PATIENT INFORMATION**

I, _____ hereby authorize UAMS to allow the entities indicated below to have access to me for the purpose of ___ photographs, ___ video recording, and ___ audio recording:

___ The UAMS Communications and Marketing Department (501)_____

MEDIA:

___ Television _____

___ Radio _____

___ Print _____

___ Other _____

In addition, I hereby authorize UAMS to release to the above-named party: (if applicable)

_____ my current treatment information

_____ my current medical condition

1. **Purpose of access or release:** At Request of Patient.
2. **Expiration Date** – This Authorization expires ninety (90) days from the date I sign the Authorization, unless I specify otherwise by writing in an earlier or later date: _____
3. **Revocation of Authorization** – I understand that I am not required to sign this Authorization. If I sign this Authorization, I may revoke the Authorization at any time by giving written notice to the UAMS Office of Communications. A revocation of this Authorization will not apply to records, information, photography, or audio/visual recordings already released in reliance upon the Authorization. A photocopy or faxed copy of this signed Authorization shall constitute a valid authorization.
4. **Release of Liability** – I agree that UAMS, including UAMS employees and attending physicians, are hereby released from legal responsibility or liability for the access provided and the release of the above information to the extent indicated and authorized herein.
5. **Re-Disclosure** – I understand that once the above information is disclosed, it may no longer be protected by privacy laws and regulations if such laws and regulations do not apply to the designated recipient, and it may be re-disclosed by the designated recipient.
6. UAMS will not condition treatment, payment, enrollment or eligibility for benefits on your signing of this Authorization.

Signature of Patient or Legal Representative _____ Date _____

If Legal Representative has signed on behalf of Patient, state the authority of Legal Representative to do so:

(such as parent of a minor, court-appointed guardian, attorney-in-fact appointed in a Power of Attorney)

Office Staff: Provide Copy of Signed Authorization to Patient/Legal Representative



UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.36

DATE: 04/01/02

REVISION: 03/01/04

SECTION: GENERAL ADMINISTRATION
AREA: ADMINISTRATION
SUBJECT: USE OF PHI FOR MARKETING

SCOPE

UAMS Workforce

PURPOSE

To establish guidelines and restrictions for the use and disclosure of Protected Health Information by UAMS in connection with marketing activities.

DEFINITIONS

For purposes of this policy, the following definitions apply:

Marketing means communications about a product or service that encourages recipients of the communication to purchase or use the product or service. Marketing also includes any arrangement between UAMS and another party in which UAMS discloses PHI for the other party to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

For purposes of this policy, “Marketing” does not include the following communications that are made by UAMS:

1. Communications by UAMS to an individual for the purpose of describing to that individual a health-related product or service that is provided by UAMS, or included in a UAMS plan of benefits; or
2. Communications by UAMS to an individual as part of the treatment of the individual; or
3. Communications by UAMS to an individual in the course of managing or coordinating treatment of that individual, or for the purpose of directing or recommending to that individual alternative treatments, therapies, health care providers, or settings of care.

Protected Health Information (PHI) means information that is part of an individual’s health information that identifies the individual or there is a reasonable basis to believe the information could be used to identify the individual, including demographic information, and that (i) relates to the past, present or future physical or mental health or condition of the individual; (ii) relates to the provision of health care services to the individual; or (iii) relates to the past, present, or future payment for the provision of health care services to an individual. This includes PHI which is recorded or transmitted in any form or medium (verbally, or in writing, or electronically). PHI excludes health information maintained in educational records covered by the federal Family Educational Rights Privacy Act and health information about UAMS employees maintained by UAMS in its role as an employer.

UAMS Workforce means for purposes of this Policy, physicians, employees, volunteers, trainees, and other persons whose conduct, in the performance of work for UAMS, are under the direct control of UAMS, whether

or not they are paid by UAMS.

POLICY

UAMS will not use or disclose a patient's Protected Health Information (PHI) for Marketing purposes except as allowed by federal and state law, including the Federal HIPAA Privacy Regulations, and any PHI that is used for disclosed by UAMS in compliance with this Policy will be limited to the minimum necessary to achieve the purpose of the use or disclosure.

PROCEDURE

- A. Prior Patient Authorization Required:** Except as allowed by this Policy, UAMS will obtain the patient's authorization in writing, using a UAMS Authorization form prior to using or disclosing a patient's Protected Health Information for Marketing purposes. See the UAMS [Use and Disclosure PHI and Medical Records Policy, 3.1.28](#) for the required elements of a HIPAA compliant authorization. If the Marketing involves direct or indirect remuneration to UAMS from a third party, the Authorization must state that such remuneration is involved.

Patient Authorization also is required prior to the use or disclosure of PHI made in connection with any arrangement between UAMS and another entity whereby UAMS discloses Protected Health Information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

This would include, for example, a situation where a company seeks access to a list of UAMS patients or any other PHI which the company will use for its own Marketing activities, regardless of whether the company is to use the PHI on behalf of UAMS as well, and seeks to do so under the guise of a Business Associate relationship or agreement. This situation requires prior patient Authorization.

- B. Prior Patient Authorization NOT Required:** UAMS is not required to obtain a written or verbal Authorization from a patient to use or disclose a patient's Protected Health Information for any Marketing communications about products or services of UAMS or a third party when the communications occur in the following circumstances:

1. face-to-face communication between UAMS and the patient (this does not include communications by telephone, e-mail or facsimile); or
2. UAMS provides to a patient a promotional gift of nominal value (e.g., items with the UAMS name or another company's name, or sample products).

- C. Communications Which are NOT Marketing, and Therefore, No Prior Patient Authorization Required:** The following types of communications made by UAMS to an individual are not considered "Marketing" for purposes of this policy, and therefore, no prior patient authorization is required:

1. Communications by UAMS to an individual for the purpose of describing to that individual a health-related product or service that is provided by UAMS, or included in a UAMS plan of benefits; or
2. Communications by UAMS to an individual as part of the treatment of the individual; or
3. Communications by UAMS to an individual in the course of managing or coordinating treatment of that individual, or for the purpose of directing or recommending to that individual alternative treatments, therapies, health care providers, or settings of care.

D. Business Associate Agreement Required: If UAMS intends to disclose Protected Health Information to a third party for the purpose of the third party communicating with individuals about the products or services of UAMS, such disclosure does not constitute Marketing communications and does not require patient Authorization. Prior to such disclosure, UAMS is required to enter into a written agreement with the third party, restricting the third party's use of the Protected Health Information to communications on behalf of UAMS and UAMS' own products and services. The agreement will be a Business Associate Agreement UAMS [Business Associate Policy, 3.1.33](#) as defined under the HIPAA regulations and approved by UAMS.

Note that the use of a Business Associate Agreement will not take the place of a patient Authorization in situations involving the use or disclosure of PHI to facilitate or conduct communications with patients about the products or services of others. This would include, for example, a situation where a company seeks access to a list of UAMS patients or any other PHI which the company will use for its own Marketing activities to promote its own products or services, regardless of whether the company is to use the PHI on behalf of UAMS as well, and seeks to do so under the guise of a Business Associate relationship or agreement. This situation requires prior patient Authorization.

E. Minimum Necessary: Any and all uses or disclosure of PHI for Marketing purposes in compliance with this Policy will be limited to the minimum necessary to achieve the purpose of the use or disclosure. UAMS [Minimum Necessary Policy, 3.1.25](#).



UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.37

DATE: 04/01/03

REVISION: 03/01/04

SECTION: GENERAL ADMINISTRATION
AREA: ADMINISTRATION
SUBJECT: VERIFICATION OF IDENTITY POLICY

SCOPE

UAMS Workforce

DEFINITIONS

The following terms have the same meaning as the terms defined in the HIPAA regulations:

Disclosure means the release, transfer, providing access to, or divulging of Protected Health Information in any manner outside of UAMS.

Protected Health Information (PHI) means information that is part of an individual's health information that identifies the individual or there is a reasonable basis to believe the information could be used to identify the individual, including demographic information, and that (i) relates to the past, present or future physical or mental health or condition of the individual; (ii) relates to the provision of health care services to the individual; or (iii) relates to the past, present, or future payment for the provision of health care services to an individual. This includes PHI which is recorded or transmitted in any form or medium (verbally, or in writing, or electronically). PHI excludes health information maintained in educational records covered by the federal Family Educational Rights Privacy Act and health information about UAMS employees maintained by UAMS in its role as an employer.

UAMS Workforce means physicians, employees, volunteers, residents, students, trainees, visiting faculty, and other persons whose conduct, in the performance of work for UAMS, is under the direct control of UAMS, whether or not they are paid by UAMS.

POLICY

Prior to disclosing any Protected Health Information, UAMS will verify the identity and authority of all individuals requesting Protected Health Information, including access to or a copy of Protected Health Information, if the identity or authority of such individuals is not known.

PROCEDURE

- A. **General -- Verification of Identity/Authority:** If the identity or authority of a person requesting PHI is not known to the UAMS workforce member responding to the request, the identity and authority of that person shall be verified prior to providing any PHI.
- B. **How to Verify Identity:** Prior to disclosing any PHI, and if identity of the person requesting PHI is not known, the UAMS workforce will request information to verify the identity of the requesting party, such as the person's valid driver's license with a photograph. To verify identity of public officials, see "Identity of Public Officials" section of this Policy.

- C. **How to Verify Authority:** The UAMS workforce will obtain any documentation, statements, or representations, whether oral or written, from the person requesting the PHI when the authority of the person to receive the PHI is not known

For Example: Prior to disclosing PHI to a person claiming to have legal authority to act on behalf of a patient, UAMS will request a copy of the document appointing the person with such legal authority, such as a Durable Power of Attorney including healthcare decisions, a Health Care Proxy appointing a person to make healthcare decisions for the patient, a court order appointing a Guardian for the patient, a court order appointing an Administrator or Executor or Personal Representative (or similar title) of the Estate of a deceased person.

- D. **Examples for Verifying Identity and Authority when it is not known to you:** Individual departments should develop procedures for verifying identity and authority that are tailored to their specific work areas. The following are examples that may be used to verify identity and authority:

1. **If the requestor is a patient:** Only the identity of the patient needs to be verified, such as a combination of full name and date of birth, and last four digits of Social Security number or other demographic information checked against documentation in our system.
2. **If the requestor is a family member:** Their name, relationship to the patient and the ability to provide specific identifying information regarding the patient may be used to verify identity. To verify authority to obtain patient information, check for documentation in the patient's record regarding their authority to receive information about the patient. If no such documentation, you may ask for the patient to call back to provide verbal permission to speak with the family member or ask for a copy of the document establishing the authority.
3. **If the requestor is a UAMS Employee:** Viewing their UAMS I.D. Badge or obtaining their name, phone number and department or UAMS billing number and determining the purpose of the request for information.
4. **If the requestor is a non-UAMS provider or other covered entity:** Their name, phone number and organization's name plus the ability to provide specific identifying information regarding the patient, and the purpose for the request, such as for treatment or payment. When in doubt call the number back or ask them to fax a written request on company letterhead.

- E. **Identity of Public Officials:** UAMS may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

1. If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status; or
2. If the request is in writing, the request is on the appropriate government letterhead; or
3. If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memoranda of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

UAMS may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, reflect that the requesting party has authority to obtain the information.

F. Authority of Public Official: UAMS may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of PHI is to a public official or a person acting on behalf of the public official:

1. A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority; or
2. If a request is made pursuant to a warrant, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, the legal authority may be presumed to exist, and the UAMS workforce must obtain a copy of the document and contact the UAMS Office of General Counsel.

G. Exceptions to Verification of Identity/Authority Requirements:

1. **Patient Directory:** UAMS is not required to verify the identity or authority of a person prior to disclosing information from the Patient Directory, as long as the patient has not opted out of the Patient Directory. If the patient has not opted out of the Patient Directory, the information which may be disclosed is limited to the patient's location in the facility and a one-word general statement of the patient's condition, and this information may be shared with any person who identifies the patient by name. See the "UAMS, 3.1.20 Release of Patient Directory Information Policy" for more information.
2. **When Patient Has Signed Authorization Form and PHI is to be Mailed:** When a patient has provided to UAMS a signed Authorization form (original or a copy) requesting release of his/her PHI to another party, and UAMS is mailing the PHI to the name and address stated in the Authorization Form, UAMS is not required to verify the identity or authority of the party designated by the patient to receive the information. (Note: The Authorization must contain the elements required by HIPAA, or the UAMS Authorization for Release of Information Form attached to the UAMS [Use and Disclosure of PHI and Medical Records Policy, 3.1.28](#), must be used.)
3. **When Patient Has Signed Authorization Form and PHI is to be Released Over the Phone or Picked Up, Verify Identity, but Not Authority:** When a patient has provided to UAMS a signed Authorization Form (original or a copy) requesting release of his/her PHI to another party, and UAMS is to release the information over the phone, or the information is to be picked up by the designated party, UAMS is not required to verify the authority of the party designated by the patient to receive the information. The authority of that person is created by virtue of the patient designating the person in the Authorization Form. However, the identity of the person must be verified to confirm that the person requesting the PHI by phone or in person is the same person who is named in the patient's authorization form.

For example: UAMS may request to see a valid driver's license with the person's picture to verify their identity. (Note: The Authorization Form must contain the elements required by HIPAA, or the UAMS Authorization for Release of Information form attached to the UAMS Use and Disclosure of PHI and Medical Records Policy must be used.)

4. **Verifying Identity/Authority of Family/Friends Involved in Care When Patient Present:** As long as the patient's identity is known, UAMS workforce are not required to verify the identity or authority of person that the patient identifies as being a member of the patient's family, a friend or other person directly involved in the patient's care, and the patient is present on the phone or in person when the identification is made.

For example: If a family member calls for PHI, and the patient is present during the phone call and informs the UAMS workforce member on the phone that UAMS can share the PHI being requested with the family member, UAMS is not required to verify the identity or authority of the family member at that time. In this circumstance, UAMS would verify that it is the patient who is on the phone, but would not need to verify the identity or authority of the family member. See UAMS [Use and Disclosure of PHI and](#)

[Medical Records Policy, 3.1.28](#) regarding disclosures to family/friends involved in patient's care for more information.

If the friend or family member claims to be a legal representative or otherwise has some type of legal authority to act on behalf of the patient in the patient's absence, this is a different situation, and UAMS will refer to the Use and Disclosure of PHI and Medical Records Policy regarding legal representatives, and also refer to the "Verification of Authority" Section C of this Policy.



UAMS ADMINISTRATIVE GUIDE

NUMBER: 3.1.40

DATE: 04/01/05

REVISION:

SECTION: ADMINISTRATION

AREA: GENERAL ADMINISTRATION

SUBJECT: WORKING FROM HOME

SCOPE

UAMS Workforce with Access to Confidential Information, including Electronic Protected Health Information (ePHI), for any purpose.

DEFINITIONS

UAMS Workforce means employees physicians, volunteers, residents, students, trainees, visiting faculty, and other persons whose conduct, in the performance of work for UAMS, is under the direct control of UAMS, whether or not they are paid by UAMS.

Confidential Information includes information concerning UAMS research projects, confidential employee information, information concerning the UAMS research programs, proprietary information of UAMS, and sign-on and password codes for access to UAMS computer systems. Confidential information shall include Protected Health Information.

Protected Health Information (PHI) means information that is part of an individual's health information that identifies the individual or there is a reasonable basis to believe the information could be used to identify the individual, including demographic information, and that (i) relates to the past, present or future physical or mental health or condition of the individual; (ii) relates to the provision of health care services to the individual; or (iii) relates to the past, present, or future payment for the provision of health care services to an individual. This includes PHI which is recorded or transmitted in any form or medium (verbally, or in writing, or electronically). PHI excludes health information maintained in educational records covered by the federal Family Educational Rights Privacy Act and health information about UAMS employees maintained by UAMS in its role as an employer.

Electronic Protected Health Information (ePHI) means individually identifiable health information that is:

- Transmitted by electronic media
- Maintained in electronic media

Information Systems means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, application, communications, and people.

POLICY

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 Protected Health Information (PHI) and Electronic Protected Health Information (ePHI) and for

following all UAMS policies and procedures related to Confidential Information, PHI, and ePHI.

PROCEDURE

1. 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.
2. The Workforce member is responsible for maintaining the privacy and security of all Confidential Information that they may be transporting, storing or accessing off-site. This includes, but is not limited to:
 - A. Protected Health Information and Electronic Protected Health Information
 - B. Computers that contain or access Confidential Information
 - C. Confidential Working Papers
3. UAMS policies are in effect whether the Workforce member is working off-site or in a UAMS facility. The following safeguards must be acknowledged:
 - A. IT Network Security 7.3.08
 1. Any Confidential Information or ePHI sent from workstations, laptops, PDAs and other mobile devices must be encrypted.
 - B. Safeguarding PHI Policy 3.1.38
 1. Electronic media and printed information must be transported and stored in a secure manner.
 2. All media containing PHI or ePHI must be disposed of appropriately and must never be placed in regular trash. This includes printed information, faxes, hard drives, diskettes and CDs.
 3. UAMS materials must be put away when not being used and kept in a secure location that is not accessible to others including children, spouse and visitors.
 - C. Mobile Device Safeguards #3.1.17 and HIPAA Security Protection from Malicious Software 7.3.15
 1. Anti-virus software must be installed on all home computers and mobile devices used for UAMS business, and they must be password protected.
 2. Employees are required to maintain updates to current operating systems (ex. Microsoft updates/patches)
 - D. Confidentiality Policy #3.1.15
 1. Passwords must not be shared or accessible to family members or others.
 - E. The printing of confidential information from home computers should be kept to a minimum and only as needed in accordance with UAMS policies.
4. UAMS Workforce Members who are assigned to work from home part-time or full-time in an official UAMS capacity involving Confidential Information must sign the formal "UAMS Work

at Home Agreement.” The agreement consists of UAMS Campus Requirements for Working from home and a section for departments to add guidelines specific to their area, if desired. For example, departments might consider including: who will bear the cost and installation of equipment, phone lines, and the replacement of any UAMS equipment that is stolen or destroyed; measures for maintaining productivity and quality; attendance at meetings; recording time worked; or other requirements.

5. UAMS will provide to the Workforce Member access to or a copy of the following UAMS Policies from the Administrative Guide:
 - A. 3.1.40 Working at Home
 - B. 3.1.15 Confidentiality Policy
 - C. 3.1.38 Safeguarding of PHI Policy
 - D. 7.3.08 IT Network Security
 - E. 3.1.17 Mobile Device Safeguards
 - F. 7.3.15 HIPAA Security Protection from Malicious Software
6. UAMS equipment taken home requires a signed UAMS Property Located Off-Campus Form.
7. Employees and/or supervisors may contact IT to verify software or hardware compliance.

UAMS Work-at-Home Agreement

UAMS Campus Requirements.

(These items must be a part of all Work-at Home Agreements)

1. I have received, agree to and abide by the following UAMS Administrative Guide Policies:
 - A. 3.1.40 Working at Home
 - B. 3.1.15 Confidentiality Policy
 - C. 3.1.38 Safeguarding of PHI Policy
 - D. 7.3.08 IT Network Security
 - E. 3.1.17 Mobile Device Safeguards
 - F. 7.3.15 HIPAA Security Protection from Malicious Software
2. I agree to maintain the privacy and security of all UAMS Confidential Information including Protected Health Information (PHI) and Electronic Protected Health Information (ePHI) and agree to access, use

and disclose in accordance with all applicable UAMS policies and procedures.

- 3. As with all UAMS workforce, I understand that my work is subject to auditing and I will cooperate with any requirements of the UAMS auditing process.
- 4. I agree to maintain current anti-virus software, spyware protection, and operating systems updates on my computer.
- 5. I understand that any violations of this agreement or UAMS policies and procedures are subject to disciplinary action up to and including termination.

.....

Department Specific Requirements, if any:

(Optional):

Employee signature

date

Employee address where work will be performed

Employee phone number

Staff:

Provide a copy of the signed agreement to the employee, a copy to UAMS OHR for the employee's personnel file, and maintain the original in the department file.