

**NUMBER: 2.1.18**

**DATE: 04/01/2003**

**REVISION: 03/01/2004; 9/23/2009; 9/08/2011; 09/04/2013**

**PAGE: 1 of 9**

---

**SECTION: HIPAA**

**AREA: HIPAA PRIVACY/SECURITY POLICIES**

**SUBJECT: BUSINESS ASSOCIATE POLICY**

---

### PURPOSE

To inform the UAMS workforce about the policy and procedure for engaging a Business Associate and executing a Business Associate Agreement.

### SCOPE

UAMS 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, provision of, access to, or divulging of information in any other manner (verbally or in writing) by UAMS to persons outside of UAMS or outside the covered components of the UAMS hybrid entity.

**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 and health information regarding a person who has been deceased for more than 50 years.

**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. For purposes of compliance with HIPAA, “Required by Law” does not automatically include a subpoena issued or signed by a non-governmental entity since certain subpoenas require that a signed HIPAA Authorization accompany the subpoena. See *Administrative Guide Policy 2.1.13, Use and Disclosure of PHI and Medical Records Policy* for more information regarding compliance with subpoenas and persons who are authorized to sign a HIPAA Authorization. .

**UAMS Workforce:** means for the purpose of this Policy, 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.

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

## **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**

### **A. 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 *Administrative Guide Policy 2.1.16, De-Identification of Protected Health Information and Limited Data Set Information*, 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 *Administrative Guide Policy 2.1.10, Minimum Necessary Policy* 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 *Administrative Guide Policy 2.1.16, De-Identification of Protected Health Information and Limited Data Set Information*, a Business Associate Agreement is not required. Only a Data Use Agreement is required.

**G. DISCLOSURES FOR PURPOSES OF RESEARCH.** See *Administrative Guide Policy 2.1.12, HIPAA Research Policy*.

**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, as well as security incident, 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, including if necessary providing the PHI in electronic format;
  - 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;

- 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;
- j. Appoint a Security Officer, have written policies and procedures in place to ensure the protection of electronic PHI, and train its workforce on its security procedures. This includes, but is not limited to, ensuring that PHI on computers and other electronic media are protected with single-user passwords and encryption;
  - i. Use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for in the Agreement. The BA will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of UAMS;
  - ii. Ensure that any agents, including a subcontractor to whom it provides protected health information, agrees to abide by the same restrictions and conditions that apply to the BA with respect to PHI, and to implement reasonable and appropriate safeguards to protect it;
  - iii. Report to UAMS HIPAA Security Officer any use or disclosure of Protected Health Information not provided for by the Agreement and any security incident of which it becomes aware;
  - iv. Maintain appropriate clearance procedures and provide supervision to assure that its workforce follows their security procedures;
  - v. Notify the UAMS HIPAA Security Officer of the termination or reassignment of any of its staff that has access to the UAMS network or servers;
  - vi. Identify and document the Business Associate's termination procedures required for removing any UAMS employee access from their applications;
  - vii. Provide appropriate training for its staff to assure that its staff complies with its security policies;

- viii. Implement appropriate security incident procedures and provide training to its staff sufficient to detect and analyze security incidents;
  - ix. Maintain a current contingency plan in case of an emergency;
  - x. If appropriate, maintain an emergency access plan to assure that the PHI it holds on behalf of UAMS is available when needed;
  - xi. Implement appropriate storage, disposal, backup, and reuse procedures to protect any PHI that the BA holds for UAMS;
  - xii. Have in place appropriate authentication and access controls to safeguard the PHI that the BA holds for UAMS;
  - xiii. Make use of appropriate encryption when transmitting PHI over the Internet and for data at rest.
- k. Not receive payment for the further disclosure of PHI without prior authorization from the patient or patient's legal representative.
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.



8. **Agreement must be validated by UAMS HIPAA Security Officer.** All potential new Business Associates must provide contact information for their HIPAA Security Officer. The UAMS Security Officer will interview potential Associates to verify the proper security controls are in place and then notify by email UAMS Contract Services and document in the HIPAA database prior to executing a Business Associate Agreement.

**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 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:

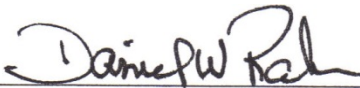
1. terminate the contract or arrangement with the Business Associate, if feasible; or if termination is not feasible, report the problem to the Secretary of the United States Department Health and Human Services; and
2. mitigate, to the extent practicable, any harm effect that is known to UAMS arising from a disclosure of PHI in violation of the UAMS policies and procedures or the HIPAA regulations.

**K. 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 Director of Contract Services, the UAMS Director of Procurement Services, or the Vice Chancellor for Finance only in their absence. 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.**

Signature: 

**Date: September 4, 2013**