PURPOSE

To inform the University of Arkansas for Medical Sciences ("UAMS") Workforce about the policy and procedures for engaging a Business Associate and executing a Business Associate Agreement.

SCOPE

UAMS Workforce.

DEFINITIONS

Business Associate shall mean 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 or provides services to UAMS* which involves disclosures that are regulated and permitted by HIPAA and which involve the creation, use or disclosure of Protected Health Information ("PHI") by the Business Associate. Business Associate functions and activities include claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. Business Associate services are legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.

Data Aggregation Services shall mean 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.

Designated Record Set shall mean 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 shall mean 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") shall mean (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 shall include 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 shall mean 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 statues 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 UAMS Administrative Guide *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 shall mean 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.

Go to the HIPAA Office website at hipaa.uams.edu to access any other terms or definitions referenced in this policy.

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.

When a vendor, consultant, company, or other outside party will receive, use, create or disclose PHI, the UAMS Agency Procurement Official will determine, in collaboration with the UAMS HIPAA Privacy Officer and UAMS HIPAA Security Officer, as may be necessary, if a Business Associate Agreement is required.

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 <u>Without</u> 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 <u>not PHI</u>, or if the PHI is de-identified in accordance with the UAMS Administrative Guide *2.1.16, De-Identification of Protected Health Information and Limited Data Set Information Policy,* 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. This contract or other written arrangement will be referred to in this Policy as a "Business Associate Agreement." The Business Associate Agreement must contain the elements specified at 45 CFR §164.504(e). The UAMS HIPAA Privacy Officer or designee must review and approve Business Associate Agreements.

D. VERIFICATION OF POTENTIAL BUSINESS ASSOCIATE. Before any Business Associate Agreement is signed and entered into, a potential new Business Associate must complete and submit to the HIPAA Security Officer a Business Associate Checklist provided by UAMS. The UAMS Security Officer will review information submitted by the potential Business Associate to verify the proper security controls are in place and then notify by email UAMS Agency Procurement Official ("APO") and document the verification in the HIPAA database. No Business Associate Agreement may be executed until the UAMS Security Officer or designee verifies and approves the potential Business Associate's security controls.

E. 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.

F. 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 Administrative Guide 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.

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

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

I. BUSINESS ASSOCIATE AGREEMENTS:

1. **Required Terms and Provisions.** A Business Associate Agreement must contain the following terms and provisions set forth in 45 CFR §164.504(e).

a. The Business Associate Agreement must establish the permitted and required uses and Disclosures of PHI by the Business Associate;

b. The Business Associate will not use or further disclose PHI other than as permitted or required by the contract or as Required by Law;

c. The Business Associate Agreement must require the Business Associate to use appropriate safeguards to prevent unauthorized use or Disclosure of the PHI, including implementing safeguards with regard to electronic Protected Health Information;

d. The Business Associate Agreement must require that the Business Associate report to UAMS any use or Disclosure of PHI not provided for by its contract, including incidents that constitute breaches or unsecured PHI, of which the Business Associate becomes aware;

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. To the extent the Business Associate is to carry out UAMS's obligation under the Privacy Rule, the Business Associate Agreement must require the Business Associate to comply with the requirements applicable to the obligation;

i. 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;

j. 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;

k. 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;

l. Authorize UAMS to terminate the contract if UAMS determines that the Business Associate has violated a material term of the contract.

2. **Optional Term and Provisions.** A Business Associate may contain other terms and provisions, including, but not limited to those listed below.

a. 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 the proper management and administration of the Business Associate; or to carry out the legal responsibilities of the Business Associate.

b. The Business Associate Agreement may permit the Business Associate to disclose PHI received by the Business Associate in its capacity as a Business Associate only if such Disclosure is necessary for the proper management and administration of the Business Associate; or to carry out the legal responsibilities of the Business Associate as long as the Business Associate, prior to disclosing PHI, 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.

c. 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 an obligation of the Business Associate under the Business Associate Agreement or other written contract evidencing the Business Associate Agreement, Business Associate 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 APO, or the Vice Chancellor for Finance only in the APO's absence. Applicable signature authority will be determined based upon type of underlying agreement.

No UAMS employee, faculty or staff member is authorized to execute a UAMS Business Associate Agreement, other than those individuals listed above.

Signature:  **Date:** **October 27, 2021**