SECTION: HIPAA
AREA: HIPAA PRIVACY/SECURITY POLICIES
SUBJECT: BREACH NOTIFICATION AND REPORTING

PURPOSE

To establish and outline Breach notification and reporting requirements at the University of Arkansas for Medical Sciences ("UAMS") and to ensure compliance with the Breach notification and reporting requirements of the Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009).

SCOPE

The UAMS Workforce.

DEFINITIONS

Breach shall mean the unauthorized acquisition, access, Use, or Disclosure of Protected Health Information which compromises the security or privacy of the Protected Health Information. Exceptions:

(i) Any unintentional acquisition, access, or Use of Protected Health Information by a UAMS Workforce member if—
- such acquisition, access, or Use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the covered entity or business associate; and
- such information is not further acquired, accessed, Used, or disclosed by any person.

(ii) Any inadvertent Disclosure from a UAMS Workforce member who is otherwise authorized to access Protected Health Information at UAMS to another similarly situated individual at UAMS; and any such information received as a result of such Disclosure is not further acquired, accessed, Used, or disclosed without authorization by any person.

(iii) An unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

Disclosure shall mean the release, transfer, provision of access to, or divulging of information in any manner (verbally or in writing) by UAMS to persons outside of UAMS or outside the covered components of the UAMS Hybrid Entity.

Legal Representative shall mean 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") shall mean 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, 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.

Secretary shall mean the Secretary of the U.S. Department of Health and Human Services or any other officer or employee of the U.S. Department of Health and Human Services to whom the authority involved has been delegated.

Unsecured Protected Health Information shall mean Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology.

Use shall mean the sharing, employment, application, utilization, examination, or analysis *within* UAMS.

UAMS Workforce shall mean 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.

Other terms or definitions referenced in this policy are available on the UAMS HIPAA Office website at hipaa.uams.edu.

POLICY

UAMS will provide notification to individuals whose Unsecured Protected Health Information has been breached as required by law. UAMS will report the same Breaches to the Secretary of the U.S. Department of Health and Human Services.

PROCEDURE

A. Internal Reporting of Breaches

1. **Reporting to the UAMS HIPAA Office:** All possible Breaches of PHI must be reported to the UAMS HIPAA Office immediately upon discovery of the Breach. Reports of Breaches by employees may be made to the following:
   - UAMS HIPAA Office, 4301 W. Markham St., Slot 829, Little Rock, AR 72205;
   - UAMS HIPAA Office (501-603-1379)

- UAMS HIPAA Inbox Email: hipaa@uams.edu;
- UAMS Compliance Reporting Line (1-888-511-3969);
- UAMS HIPAA Website at hipaa.uams.edu/ under "Report an Incident";
- UAMS Research Privacy Board Office/IRB (501-686-5667);
- UAMS Research Privacy Board Email: IRB@uams.edu or
- UAMS IT Security through Technical Support Center (501-686-8555)

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

2. **Reporting to UAMS IT Security:** All lost equipment possibly containing PHI must be reported to UAMS IT Security as soon as the loss is discovered, regardless of whether the equipment is encrypted or password protected. This includes but is not limited to all thumb drives, CDs or DVDs, computers, laptops, smartphones, and alphanumeric pagers. All reports to IT Security should be made by calling the IT Helpdesk at 686-8555. For more information, see UAMS Administrative Guide Policy 2.1.32, *Security Incident Identification and Handling Policy.*

3. **Reporting to Law Enforcement:** All thefts and suspected thefts involving PHI must be reported to law enforcement immediately upon discovery.

B. Examples of Possible Breaches and Appropriate Actions to be Taken

1. A nurse working in the hospital is searching for her patient in the electronic medical record system when she inadvertently clicks on another patient's record who has the same name as her patient. As soon as she realizes she is in the wrong patient's record, she exits the record. The nurse does not need to notify the UAMS HIPAA Office, because this does not meet the definition of a Breach.

2. A Workforce member receives notice that a fax he sent to another doctor's office was inadvertently faxed to a florist, whose fax number is one digit different from the doctor's fax number. The Workforce member must notify the UAMS HIPAA Office immediately.

3. One patient's discharge instructions are inadvertently given to another patient who is in the next exam room. The patient brings the discharge instructions back and informs the nurse that they are not his. The nurse must notify the UAMS HIPAA Office immediately.

4. A physician realizes that his smartphone is missing, and the phone contains email that may have patient information in it. He is not sure where the phone is, but he knows he has not seen it in several hours. The physician should notify IT Security and the UAMS HIPAA Office immediately.

5. The home of a research assistant who works from home is broken into and a locked file box containing patient records is stolen. The research assistant must contact law enforcement and the UAMS HIPAA Office immediately.

6. A traveling nurse's encrypted laptop containing PHI is stolen out of her car. The nurse must report the theft to law enforcement, UAMS IT Security, and the UAMS HIPAA Office immediately.

C. Retention of Documents: All documents possibly involved in the Breach should be retained and turned over to the UAMS HIPAA Office. If the documents were impermissibly disclosed to a third party, that third party should be instructed to securely maintain the documents and await instruction from the UAMS HIPAA Office.

D. Patient Notification: The UAMS HIPAA Office will determine whether a Breach has occurred based on a risk assessment of factors set forth in the HIPAA rules and regulations and will coordinate and manage all patient notifications.

1. **Notice to Patients:** The UAMS HIPAA Office will provide written notice to individuals whose Unsecured PHI has been breached, as soon as reasonably possibly, and in no case later than 60 calendar days after the Breach is discovered. The notice will contain (a) a brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known; (b) a description of the type of Unsecured PHI involved in the Breach; (c) steps the impacted individuals should take to protect themselves from potential harm resulting from the Breach; (d) a brief description of what UAMS is doing to investigate the Breach, mitigate the harm, and protect against future Breaches; and (e) contact information for the individuals to use if they have questions or need additional information, including a toll-free telephone number, and email address, web site or postal address.

2. **Notice to Personal Representatives:** If the patient is deceased, the written notice will be provided to the next of kin or personal representative, if their address is known. No substitute notice is required when there is insufficient or out-of-date contact information that precludes written notification to the next of kin or the personal representative of the deceased patient.

3. **Substitute Notice:** If the address is unknown for fewer than 10 individuals, then a substitute notice will be provided by other means reasonably calculated to reach the affected individual, such as by telephone. If the address is unknown for 10 or more individuals, then a substitute notice will be provided by either a conspicuous posting on the UAMS website for 90 days or a conspicuous publication in major print or broadcast media in the geographic areas where the individuals affected by the Breach likely reside. The posting on the UAMS website or the notice published in major print or broadcast media must include a toll-free number that remains active for at least 90 days where an individual can learn whether the individual's Unsecured PHI was included in the Breach. No substitute notice is required when there is insufficient or out-of-date contact information that precludes written notification to the next of kin or the personal representative of the affected individual who is deceased.

4. **Urgent Notice:** If the UAMS HIPAA Office determines that there is an imminent threat

that the patient's information could be misused, urgent notice may be provided via telephone or email, in addition to first class mail.

5. **Law Enforcement Delay of Notice:**

   a. **Written Statement.** If a law enforcement official states in writing to UAMS that a notification, notice or posting required pursuant to this policy would impede a criminal investigation or cause damage to national security, and the written statement specifies the time for which a delay is required, UAMS shall delay such notification, notice or posting for the time period specified by the law enforcement official.

   b. **Oral Statement.** If a law enforcement official orally states to UAMS that a notification, notice or posting required pursuant to this policy would impede a criminal investigation or cause damage to national security, UAMS shall document the oral statement, including the identity of the law enforcement official making the oral statement, and shall delay the notification, notice or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time that meets the requirements in section above.

6. **Notice to Media:** If the Breach involves (or is reasonably believed to have involved) more than 500 residents in a state or jurisdiction, prominent media outlets serving that state or jurisdiction will also be notified. The notice will be provided in the same time frame as provided to the affected individuals and must contain the same content as the notice to the affected individuals. The UAMS HIPAA Office will work with the UAMS Office of Communications to notify the media of a Breach, as may be required. The UAMS Office of Communications will be responsible for all contact with the media.

7. **Out of State Notice:** When notice is required to patients who are residents of another state, the HIPAA Office will comply with all state Breach notification requirements that are more stringent than the HIPAA requirements, if necessary.

E. **Breach Reporting to the U.S. Department of Health and Human Services:** The UAMS HIPAA Office will report to the Secretary of the U.S. Department of Health and Human Services all discovered Breaches of Unsecured PHI. If the Breach involves 500 or more individuals, the UAMS HIPAA Office will report to the Secretary at the same time as the affected individuals. For Breaches that involve fewer than 500 individuals, the UAMS HIPAA Office will maintain a log of the Breaches and, no later than 60 days after the end of each calendar year, will report to the Secretary Breaches discovered in the preceding calendar year in the manner specified on the U.S. Department of Health and Human Services web site.

F. **Mitigation:** The UAMS HIPAA Office will, with assistance from IT Security and the department involved in the incident, identify and implement any mitigation steps may be necessary, including but not limited to notifying law enforcement, activating remote control over a device, requesting that PHI be returned or destroyed by the recipient, additional training, changes to policies and procedures, and notifying the patient(s) involved.

G. 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 in accordance with terms and provisions of the agreement or contract. Refer to UAMS Administrative Guide Policy 2.1.18, *Business Associate Policy.*

SANCTIONS

Violation of this Policy will result in disciplinary action, in accordance with UAMS Administrative Guide Policy 4.4.02, *Employee Discipline* and UAMS Administrative Guide Policy 2.1.42*, HIPAA Sanctions Policy.*

Signature:  **Date: December 9, 2020**