

NUMBER: 2.1.08**DATE: 04/01/2003****REVISION: 4/29/09; 6/7/11; 8/7/13; 9/3/14; 3/27/19; 7/10/19; 11/09/20; 02/07/2023** **PAGE: 1 of 2****SECTION: HIPAA****AREA: HIPAA PRIVACY/SECURITY POLICIES****SUBJECT: REPORTING OF HIPAA VIOLATIONS****PURPOSE**

To inform the University of Arkansas for Medical Sciences (“UAMS”) Workforce on the proper procedure for reporting violations of the Health Insurance Portability and Accountability Act (“HIPAA”).

SCOPE

The UAMS Workforce.

DEFINITIONS

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

POLICY

Any known or suspected violation of the HIPAA regulations or related UAMS policies and procedures are to be reported immediately. UAMS Workforce members 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.

PROCEDURE**A. Reporting Possible HIPAA Violations**

Members of the UAMS Workforce must report suspected HIPAA violations immediately. Patients may also report possible violations. Reports may be made to any of the following:

- UAMS HIPAA Office, 4301 West Markham St. Slot 829, Little Rock, AR 72205;
- UAMS HIPAA Office, MAIN OFFICE (501-603-1379);
- UAMS HIPAA Inbox Email: hipaa@uams.edu;
- UAMS 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), Email: IRB@uams.edu; or
- UAMS IT Security through Technical Support Center (501-686-8555).

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

B. Mitigation

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

C. HIPAA Violations by Business Associates or Contractors

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 may terminate the Business Associate or Contractor relationship in accordance with the terms and provisions of the contract or agreement. 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 4.4.02, *Employee Discipline Policy* and UAMS Administrative Guide 2.1.42, *HIPAA Sanctions Policy*.

Signature: 

Date: February 7, 2023