

NUMBER: 2.1.25**DATE: 04/23/2009****REVISION: 01/18/2017****PAGE: 1 of 2****SECTION: HIPAA****AREA: HIPAA PRIVACY/SECURITY POLICIES****SUBJECT: IDENTITY THEFT PREVENTION****PURPOSE**

To prevent and detect identity theft involving UAMS Covered Accounts and comply with the Trade Commission's Red Flags Rule, this policy implements UAMS's Identity Theft Prevention Program ("Program").

SCOPE

This Policy applies to UAMS patient and student records that are associated with Covered Accounts.

DEFINITIONS

Covered Account means any Account UAMS offers or maintains that involves multiple payments or transactions, or for which there is a foreseeable risk of Identity Theft.

Identifying Information for purposes of the Program means any name or number that may be used alone or in conjunction with any other information to identify a specific person. Examples of "identifying information" include name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, unique electronic identification number, computer's Internet Protocol address, or routing code.

Identity Theft means fraud committed using the "Identifying Information" of another person.

Red Flag means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft examples include documents provided for identification that appear to have been altered or forged, information on identification documents is not consistent with information that is on file with UAMS, the information on multiple identification documents provided is not consistent, the Social Security Number provided is the same as that submitted by another patient, and a patient notifies UAMS that he may potentially be a victim of identity theft.

POLICY

As required by the Federal Trade Commission's Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003, 16 C.F.R. § 681.2, UAMS will maintain an Identity Theft Prevention Program. As part of the Program, UAMS will identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program; detect Red Flags that have been incorporated into the Program; respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and

ensure the Program is updated periodically to reflect changes in risks to patients and students or to the safety and soundness of UAMS from Identity Theft.


PROCEDURE

1. **Oversight.** Responsibility for developing, implementing and updating the Program shall lie with a Program Administrator who is appointed by the Vice Chancellor for Institutional Compliance. The Program Administrator reports annually to the Board of Trustees or the Vice Chancellor for Institutional Compliance regarding an evaluation of how effective the Program has been in addressing the risk of Identity Theft, how UAMS is monitoring the practices of service providers, significant incidents of identity theft and the response, and recommendations for material changes to the Program.
2. **Implementation of the Identity Theft Prevention Program.** The Program Administrator may work with representatives from Hospital Admissions, Patient Billing Services, Faculty Group Practice billing, Health Information Management, representatives involved with student records, and others as may be necessary to implement the Program. Processes necessary to detect the Red Flags named in the Program and to prevent and mitigate Identity Theft are identified and implemented in the appropriate departments at the direction of the Program Administrator. Appropriate responses to prevent and mitigate Identity Theft may include contacting the patient, alerting UAMS employees, faculty and staff that a Covered Account may involve possible Identity Theft, requiring specific forms of identification to authenticate the individual, notifying law enforcement, or determining that no response is warranted under the particular circumstances.
3. **Training.** UAMS staff responsible for implementing the Program shall be trained, as applicable to their job function, either by or under the direction of the Program Administrator. Program implementation training shall consist, in part, on the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. The Program Administrator may delegate training for new employees, refresher training as needed, and training on new policies or procedures when the Program is updated.
4. **Provider Agreements.** UAMS will review its agreements with service providers who perform services in connection with Covered Accounts to ensure that the providers have reasonable policies in place to detect, prevent, and mitigate the risk of Identity Theft. UAMS will, as necessary, require, by contract that service providers have such policies and procedures in place, and UAMS will require, by contract, that service providers report any Red Flags to the Program Administrator.

REFERENCES

See also the [Arkansas Personal Information Protection Act](#).

University of Arkansas for Medical Sciences Identity Theft Prevention Program

Signature:  _____

Date: January 18, 2017