



UNIVERSITY OF ARKANSAS  
FOR MEDICAL SCIENCES

## UAMS ADMINISTRATIVE GUIDE

**NUMBER: 3.1.43**

**DATE: April 23, 2009**

**REVISION:**

**PAGE: 1 of 2**

**SECTION: Administration**

**AREA: General Administration**

**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.

### **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 an Identity Theft Prevention Committee. The Committee is headed by a Program Administrator who is appointed by the Vice Chancellor for Institutional Compliance. In addition to the Program Administrator, the Committee will consist of representatives from Hospital Admissions, Patient Billing Services, Faculty Group Practice billing, Health Information Management, and a representative involved with student records.
2. **Implementation of the Identity Theft Prevention Program.** The Identity Theft Prevention Committee will implement the Program by identifying processes necessary to detect the Red Flags named in the Program and to prevent and mitigate Identity Theft. The Committee members will implement these processes in their respective departments at the direction of the Program Administrator.
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.

SIGNATURE:



Chancellor

Date: April 23, 2009