KALEIDA HEALTH

POLICY/ PROCEDURE/PROTOCOL

Title: Identity Theft Prevention: Red Flag Program									**Policy # ADM.14**	
Audience: Corporate										
Key Word: identity theft, red flag, fraud									**Date Issued:** 2/16/09	**Page:** **1 of 4**
Distribution: All holders of the policy and procedure manual										
Prepared by: Internal Audit & Corporate Compliance Patient Financial Services Patient Access Laboratory Services Legal Services Risk Management Health Information Management IS Security									**Effective Date:** 2/21/11	
Approved by: Legal Counsel Audit & Corporate Compliance Committee									**Date:** 1/15/09, 1/26/11 2/3/09	
Regulation/ Standards- NYS: N/A Federal: 16 CFR § 681; 16 CFR § 603.2(a) Accreditation Standards: N/A										
Review Date	1/10	1/11								
Revision Date		1/11								

I. Introduction

"Identity theft" means fraud committed using the identifying information of another person. "Medical identity theft" refers to the misuse of another individual's personally identifiable information such as name, date of birth, social security number, or insurance policy number, to obtain or bill for medical services or medical goods.[1] Medical identity theft frequently results in erroneous entries being put into existing medical records, and can involve the creation of fictitious medical records in the victim's name.[2] Kaleida Health is committed to monitoring for the potential that patients may be victims of identity theft, and maintaining a process to mitigate this risk.

II. Communication and Responsibility

All Corporate, Division, Administrative Officers, and Department Heads in conjunction with the Supervisors and Managers of Health Information Management, Patient Financial Services, Patient Access and IS&T.

III. Scope of Practice

This policy and procedure applies to all Medical Staff members, hospital staff, clinic, home care staff, nursing home staff, and corporate support staff at Kaleida Health, including employees, students, interns, residents and volunteers. It also governs consultants, contractors and vendors of Kaleida Health, as applicable. For purposes of this policy, the term "hospital staff"

shall include home care and nursing home staff, and the term "hospital" shall include Kaleida Health home care and skilled nursing facilities.

IV. Policy

A. **Definitions**

For the purposes of the Program, the following terms are defined as:

1. "Covered account" means (a) any account Kaleida Health offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions, including one or more deferred payments; and (b) any other account Kaleida Health identifies as having a reasonably foreseeable risk to customers or to the safety and soundness of Kaleida Health from identity theft. As of the effective date of this policy, Kaleida Health has identified the following types of accounts as covered accounts:
   a. Patient/Client/Resident accounts
   b. Billing records
   c. Pharmacy records
   d. Vendor accounts
   e. Accounts for research projects.

2. "Customer" means a person that has a covered account.

3. "Fraud" means a deception deliberately practiced in order to secure unfair or unlawful gain.

4. "Red flag" means a pattern, practice or specific activity that indicates the possible existence of identity theft.

5. "Service provider" means a person that provides a service directly to Kaleida Health.

B. **Purpose**

The purpose of this program is to:

1. Identify relevant red flags based on the risk factors associated with Kaleida Health's covered accounts, as determined by a committee made up of representatives from Internal Audit & Corporate Compliance, Patient Financial Services, Health Information Management, Patient Access, Laboratory Services, Legal Services, Risk Management and IS Security;
2. Institute procedures for detecting red flags;
3. Identify steps to be taken to prevent and mitigate identity theft; and
4. Create a system for regular updates and administrative oversight of the Red Flag Program.

C. **Identification of relevant red flags**

The Identity Theft Mitigation and Resolution Procedures outlined in **Attachment A** identify the red flags that would be most relevant to Kaleida Health, as determined by a committee made up of representatives from Internal Audit & Corporate Compliance, Patient Financial Services, Health Information Management, Patient Access, Laboratory Services, Legal Services, Risk Management and IS Security. Red flags generally will fall into one of the following general categories:

1. Suspicious documents;
2. Suspicious personal identifying information;

3. Suspicious or unusual use of covered accounts; and
4. Alerts from others (for example, a patient/client/resident or his/her representative, an identity theft victim, law enforcement, etc.)

D. **Detection of red flags**

In order to facilitate detection of the red flags identified in **Attachment A**, Kaleida Health will take the following steps to obtain and verify the identity of the person:

1. New patient/client/resident accounts:
   a. Request identifying information (ex., full name, date of birth, address, insurance card, government issued ID, etc.)
   b. When available, verify information with insurance company's information
2. Existing accounts:
   a. Verify identification of patients/clients/residents or their representatives before giving out any personal information
   b. Verify identification of patients/clients/residents or their representatives before accommodating requests for changes of billing address

E. **Prevention and mitigation of identity theft**

In order to prevent and mitigate the effects of identity theft, Kaleida Health will follow the appropriate steps identified in the Identity Theft Mitigation and Resolution Procedures outlined in **Attachment A**. Kaleida Health's Office of General Counsel will review incidents to determine events of actual or potential fraud.

F. **Updating of the program**

A committee made up of representatives from Internal Audit & Corporate Compliance, Patient Financial Services, Health Information Management, Patient Access, Laboratory Services, Legal Services, Risk Management and IS Security will be responsible for updating the Red Flag Program.

G. **Service provider arrangements**

Kaleida Health will require, by contract, that service providers that perform activities in connection with covered accounts have policies and procedures in place designed to detect, prevent and mitigate the risk of identity theft with regard to the covered accounts.

H. **Administrative oversight**

Staff will be trained, as necessary, to effectively implement the Red Flag Program. At a minimum, such training will be done on hire and annually thereafter.

V. Procedure – **See Attachment A**.

VI. Protocol – N/A

VII. Documentation

A committee made up of representatives from Internal Audit & Corporate Compliance, Patient Financial Services, Health Information Management, Patient Access, Laboratory Services, Legal Services, Risk Management and IS Security will be responsible for maintaining documentation of triggered red flags.

VIII. References

[1] Booz Allen Hamilton. "Medical Identity Theft Environmental Scan." United States Department of Health and Human Services, Office of the National Coordinator for Health Information Technology. October 2008.

[2] Dixon, Pam. "Medical Identity Theft: The Information Crime That Can Kill You." World Privacy Forum. May 3, 2006.