

RED FLAGS IDENTITY THEFT PREVENTION PROGRAM

Because they are likely to meet the Red Flags Rule's broad definition of "creditor" and have patient accounts that fall within the scope of "covered account," hospitals must develop a written identity theft prevention program. The FTC recently announced that it will *suspend enforcement* of the rule until May 1, 2009 to give hospitals and other organizations that are subject to FTC's regulatory oversight additional time to develop and implement their programs. However, the compliance deadline remains November 1, 2008 and hospitals should make a good faith effort to be in compliance with the rule's requirements as soon as possible.

To get hospitals started in developing their written identity theft programs, the AHA in cooperation with its outside counsel Hogan & Hartson LLP developed a sample policy that hospitals can use as a first step in developing and implementing a program that is responsive to the specific operations and needs of their individual organizations.

The final regulations state that an identity theft program "must be appropriate to the size and complexity of the [covered entity] and the nature and scope of its activities." ***While it may be appropriate to start with a sample policy, each organization must adapt the sample document to address the specific risks to their patient and other covered accounts and to ensure an appropriate and reasonable response to those risks.***

The sample policy is not intended to, and cannot, substitute for responsible legal advice. Hospitals should examine the sample document as part of a comprehensive risk assessment. Hospitals already may have processes and procedures in place to detect and respond to cases of potential identity theft and they will want to incorporate these existing activities into their individual organization's policy. Additionally, suggested guidelines for developing and structuring an identity theft program are included in the final rule's Appendix A, which starts on page 63773, and the supplement to the appendix identifies 26 potential red flags. While not all of the guidelines or red flags may be directly applicable to health care organizations, hospitals, *as the FTC has specifically urged*, should carefully consider and evaluate whether and how to incorporate them into their organization's policies and identity theft programs.

Hospitals also should carefully consider how compliance with other current federal and state legal requirements may impact the organization's identity theft policy. For example, EMTALA's obligations to provide without delay medical screening and stabilizing treatment for emergency medical conditions may affect policies related to verification of patient identity in the emergency department. HIPAA's privacy requirements will affect the design of policies that involve access to and sharing of patient information. State law security breach notification requirements may determine the reasonable response to an identified red flag.

SAMPLE
FOR CONSIDERATION ONLY

The rule requires that organizations periodically reassess and revise their policies and practices, including modifications and/or expansions to detect and respond to new and emerging risks. Hospitals will want to specifically charge someone within the organization with responsibility for maintaining and updating the program and policies and include such effort as an explicit component of the program from the start.

SAMPLE POLICY
RED FLAGS IDENTITY THEFT PREVENTION PROGRAM
[DATE]

[items to be modified are in italics and brackets]

The Board of [Directors/Trustees] of [HOSPITAL] (“Hospital”) approved this Identity Theft Prevention Program (“Program”) at a duly held meeting on _____, 2008. The Program was developed in order to comply with the Federal Trade Commission’s Identity Theft Prevention Red Flags Rule (16 CFR § 681.2). This Program has been created in consultation with [INSERT RELEVANT GROUPS AND DIVISIONS], [Patient Billing, IT, Medical Records, and the Legal Department], after conducting an assessment of risk of Identity Theft associated with certain Covered Accounts (as defined below) offered by the Hospital.

I. Definitions

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

“Covered Account” means (i) any account Hospital offers or maintains primarily for personal family or household purposes, that involves multiple payments or transactions, including one or more deferred payments; and (ii) any other account the Hospital identifies as having a reasonably foreseeable risk to customers or to the safety and soundness of the Hospital from Identity Theft. As of _____, the Hospital has identified the following [four] types of accounts as Covered Accounts

- 1) [non-emergency patient billing]
- 2) [patient payment plan]
- 3) [INSERT TYPES OF PLANS THAT HAVE DEFERRED PAYMENTS]__
- 4) _____

“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

II. Program Purposes

The purposes of the Program are to:

- 1) Identify the relevant Red Flags based on the risk factors associated with the Hospital’s covered accounts;
- 2) Institute policies and procedures for detecting Red Flags;
- 3) Identify steps the institution will take to prevent and mitigate Identity Theft; and
- 4) Create a system for regular updates and administrative oversight to the Program.

SAMPLE
FOR CONSIDERATION ONLY

III. Identification of Red Flags

The Identity Theft Red Flags Mitigation and Resolution Procedures (Appendix A) identifies the Red Flags that would be most relevant to the Hospital. The Red Flags generally fall within one of the following *[four]* general types of Red Flags:

- 1) Suspicious Documents;
- 2) Suspicious Personal Identifying Information;
- 3) Suspicious or Unusual Use of Covered Account; and
- 4) Alerts from Others (e.g. customer, Identity Theft victim, or law enforcement)

IV. Detection of Red Flags

In order to facilitate detection of the Red Flags identified in Appendix A, *[appropriate Hospital staff]* will take the following steps to obtain and verify the identity of the person.

A. New Patients/Accounts

- 1) Require identifying information (e.g., full name, date of birth, address, government issued ID, insurance card, etc.)
- 2) When available, verify information with insurance company's information
- 3) *[IF YOU RUN A CREDIT CHECK, MENTION THAT HERE]*

B. Existing Accounts

- 1) Verify validity of requests for changes of billing address
- 2) Verify identification of customers before giving out any personal information

V. Preventing and Mitigating Identity Theft

In order to prevent and mitigate the effects of Identity Theft, staff will follow the appropriate steps identified in the attached Identity Theft Red Flags Mitigation and Resolution Procedures (Appendix A).

VI. Program Administration

The *[insert title of responsible individual or committee]* is responsible for developing, implementing, administering and updating the Program. *[TITLE]* will be responsible for developing a training program for staff identified by *[TITLE]* as responsible for or having a role in implementing the Program.

VII. Service Provider Arrangements

Hospital 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.

VII. Updating of Program

The *[INSERT RESPONSIBLE PERSON OR GROUP]* will periodically review the effectiveness of the Program and update the Program to reflect the addition or removal of Covered Accounts, and changes in risks to patients/covered account holders from Identity Theft.

SAMPLE

Attachment A
Relevant Identity Theft Red Flags Mitigation and Resolution Procedures

IDENTITY THEFT RED FLAG	PREVENTION/MITIGATION PROCEDURE	RESOLUTION OF RED FLAG [ONLY SUGGESTIONS]
Documents provided for identification appear to have been altered or forged.	Stop the admissions/billing process and require applicant to provide additional satisfactory information to verify identity.	Additional documentation must be provided to resolve discrepancy and continue admissions/billing process.
Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the patient. For example, there is a lack of correlation between the Social Security Number (SSN) range and date of birth.	Stop the admissions/billing process and require applicant to provide additional satisfactory information to verify identity.	Additional documentation must be provided to resolve discrepancy and continue admissions/billing process.
The SSN provided is the same as that submitted by other persons opening an account or other customers.	Stop the admissions/billing process and require applicant to provide additional satisfactory information to verify identity.	Additional documentation must be provided to resolve discrepancy and continue admissions/billing process.
Patient has an insurance number but never produces an insurance card or other physical documentation of insurance.	Stop the admissions/billing process and require applicant to provide additional satisfactory information to verify identity.	Additional documentation must be provided to resolve discrepancy and continue admissions/billing process. Contact insurance company as necessary. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.

SAMPLE
FOR CONSIDERATION ONLY

<p>Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient (e.g., inconsistent blood type).</p>	<p>Investigate complaint, interview individuals as appropriate, review previous files for potential inaccurate records. Items to consider include: blood type, age, race, and other physical descriptions may be evidence of medical identity theft.</p>	<p>Depending on the inconsistency and review of previous file, either delay/do not open a new covered account, or terminate services.</p> <p>If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.</p>
<p>Complaint/inquiry from an individual based on receipt of: -a bill for another individual -a bill for a product or service that the patient denies receiving -a bill from a health care provider that the patient never patronized - a notice of insurance benefits (or Explanation of Benefits) for health services never received.</p>	<p>Investigate complaint, interview individuals as appropriate</p>	<p>Terminate treatment/credit until identity has been accurately resolved; refuse to continue attempting to collect on the account until identity has been resolved.</p> <p>Notify law enforcement as appropriate.</p> <p>If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.</p>
<p>Complaint/inquiry from a patient about information added to a credit report by a health care provider or insurer</p>	<p>Investigate complaint, interview individuals as appropriate</p>	<p>Terminate treatment/credit until identity has been accurately resolved; refuse to continue attempting to collect on the account until identity has been resolved.</p> <p>Notify law enforcement as appropriate.</p> <p>If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.</p>
<p>Complaint or question from a patient about the receipt of a</p>	<p>Investigate complaint, interview individuals as appropriate</p>	<p>Terminate treatment/credit until identity has been accurately resolved; refuse</p>

SAMPLE
FOR CONSIDERATION ONLY

<p>collection notice from a bill collector.</p>		<p>to continue attempting to collect on the account until identity has been resolved.</p> <p>Notify law enforcement as appropriate.</p> <p>If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.</p>
<p>Patient or insurance company report that coverage for legitimate hospital stays is denied because insurance benefits have been depleted or a lifetime cap has been reached.</p>	<p>Investigate complaint, interview individuals as appropriate</p>	<p>Additional documentation must be provided to resolve discrepancy and continue admissions/billing process. Contact insurance company as necessary.</p> <p>Notify law enforcement as appropriate.</p> <p>If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.</p>
<p>Mail sent to the patient is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the patient's covered account.</p>	<p>Skip-tracing procedures are used to find the patient's current mailing address.</p>	<p>Patient is found and contact information is updated.</p>
<p>Hospital is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.</p>	<p>Investigation to determine if billing was made fraudulently.</p>	<p>Additional documentation must be provided to resolve discrepancy and continue admissions/billing process. Contact insurance company as necessary.</p> <p>Notify law enforcement as appropriate.</p>

SAMPLE
FOR CONSIDERATION ONLY

		<p>If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.</p>
<p>Personal identifying information provided by the patient is associated with known fraudulent activity as indicated by internal or third-party sources used by the Hospital. For example:</p> <ul style="list-style-type: none"> - The address on an application is the same as the address provided on a fraudulent application; or - The phone number on an application is the same as the number provided on a fraudulent application. 	<p>Investigate complaint, interview individuals as appropriate</p>	<p>Terminate treatment/credit until identity has been accurately resolved; refuse to continue attempting to collect on the account until identity has been resolved.</p> <p>Notify law enforcement as appropriate.</p> <p>If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.</p>