	Information Security Policy	No. COMP-Sec 4.1.3
	Title:	Page: 1 of 6
	IDENTITY THEFT PREVENTION PROGRAM (RED FLAG RULE)	Effective Date: 05-01-2009
		Retires Policy Dated:
		Previous Versions Dated:

I. SCOPE:


This policy applies to (1) Tenet Healthcare Corporation and its wholly-owned subsidiaries and affiliates (each, an “Affiliate”); (2) any other entity or organization in which Tenet Healthcare Corporation or an Affiliate owns a direct or indirect equity interest of 50% or more; and (3) any hospital or healthcare facility in which Tenet Healthcare Corporation or an Affiliate either manages or controls the day-to-day operations of the facility (each, a “Tenet Facility”) (collectively, “Tenet”).

II. PURPOSE:

The purpose of this policy is to define Tenet’s responsibilities in detecting, preventing, and mitigating identity theft as required by the Federal Trade Commission (FTC) under the Fair and Accurate Credit Transactions (FACT) Act. The rule adopted by the FTC is referred to as the “Red Flag Rule.” The risk to Tenet, its employees and patients from data loss and identity theft is of significant concern to Tenet and can be reduced only through the combined efforts of every employee and contractor.

III. DEFINITIONS:

- A. “**Covered Accounts**” means any account offered by a creditor that is primarily used for personal, family, or household purposes involving (or is designed to permit) multiple payments or transactions.
- B. “**Creditor**” means any person or entity who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.
- C. “**Identity Theft**” means fraud committed using the identifying information of another person.
- D. “**Red Flag**” means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.
- E. “**Sensitive Information**” means information about employees or patients as follows.
 - 1. Name
 - 2. Social Security Number
 - 3. Date of birth


	Information Security Policy	No.	COMP-Sec 4.1.3	
	Title:	Page:	2 of 6	
	IDENTITY THEFT PREVENTION PROGRAM (RED FLAG RULE)	Effective Date:	05-01-2009	
		Retires Policy Dated:		
		Previous Versions Dated:		

4. Driver's license or government identification number
5. Alien Registration Number
6. Passport number
7. Employer or taxpayer identification number
8. Credit card and bank account number
9. Home address
10. Billing address
11. Telephone numbers
12. Patient account numbers
13. Payment status

F. **"Service Provider"** means a person that provides a service directly to the creditor.


IV. POLICY:

- A. Tenet's Identity Theft Task Force ("Task Force") shall be chaired by the Chief Compliance Officer (CCO) or designee and shall include, at a minimum, the Director of Privacy and Security Compliance, the Director of IS Security, the Director of Audit Services, Law Department Regulatory Counsel, Law Department Human Resources Counsel and Corporate Communications. The Task Force provides oversight to ensure that Tenet operates in compliance with the regulatory requirements of the Red Flag Rule and other federal and state privacy and Identity Theft laws. The Task Force oversees the effectiveness of the Identity Theft Prevention Program (the "Program") and makes decisions on effectiveness of the Program which are communicated to the CCO. The Task Force also provides the oversight of all Identity Theft policies and procedures. The Task Force shall monitor, with input from Tenet Facilities, all Identity Theft-related incidents. The Task Force shall meet at least quarterly.
- B. All employees, contractors, and Service Providers are expected to report potential Identity Theft incidents involving Highly Sensitive Information and Sensitive Information immediately upon discovery or notification of the same. Reports should be made to an immediate supervisor, department director, Hospital Compliance/Privacy Officer (HCO), Information Security Officer (ISO), Chief Compliance Officer (CCO), or designee, or the Ethics Action Line (EAL). If

	Information Security Policy	No.	COMP-Sec 4.1.3	
	Title:	Page:	3 of 6	
	IDENTITY THEFT PREVENTION PROGRAM (RED FLAG RULE)	Effective Date:	05-01-2009	
		Retires Policy Dated:		
		Previous Versions Dated:		

reports are made to a supervisor or department director, that individual is expected to immediately forward the report to the HCO or CCO.

- C. Upon receipt of a report of a potential Identity Theft incident, the Task Force shall make a preliminary, good faith inquiry into the allegations to ensure that all of the information necessary to determine whether a further review should be conducted has been obtained.
- D. Individuals who report a potential Identity Theft incident shall not face retribution or retaliation. Allegations of retaliation will be investigated and addressed according to Human Resources Policy HR-116 No Retaliation. In addition, to the extent possible and if allowed by law, the anonymity of the individual reporting the potential Identity Theft incident will be protected.
- E. At the facility level, the HCO is designated as the preferred internal contact for the reporting of potential Identity Theft incidents for that facility. Supervisors or department directors who become aware of a potential Identity Theft incident should report it to the HCO immediately at the time the incident is identified. It is the responsibility of the facility A-team and HCO to ensure adherence to this policy.
- F. All facilities are required to submit an annual report to their facility Governing Board/Board of Directors or an appropriate committee of the Board and the Task Force. Facilities without a Governing Board/Board of Directors shall submit an annual report to Tenet Facility senior management. The report shall address the oversight and effectiveness of the program, the effectiveness of the policies and procedures, a summary of any identify theft incidents and the response to the incident, and recommendations for substantial changes to the program, if any.
- G. The original reports will be maintained by the HCO at the facility and will be made available for inspection by members of the Hospital Compliance Committee and/or other appropriate Tenet representatives.
- H. Training shall be conducted for all employees, officials and contractors for whom it is reasonably foreseeable that they may come into contact with Covered Accounts or personally identifiable information that may constitute a risk to Tenet or its employees or patients. To ensure maximum effectiveness, employees may continue to receive additional training as changes to the program are made.
- I. The initial written Program must be approved by either the Governing Board/Board of Directors or an appropriate committee of the Board. If the Tenet Facility does not have a Governing Board or Board of Directors, the initial written Program must be approved by Tenet Facility senior management.

	Information Security Policy	No.	COMP-Sec 4.1.3	
	IDENTITY THEFT PREVENTION PROGRAM (RED FLAG RULE)	Title:	Page:	4 of 6
		Effective Date:	05-01-2009	
		Retires Policy Dated:		
		Previous Versions Dated:		

V. PROCEDURE:

A. Identification of Red Flags

The Identity Theft Red Flags Mitigation and Resolution Procedures (Attachment A) identifies the Red Flags that would be most relevant to the Tenet Facility. The Red Flags generally fall within one of the following four 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. patient, Identity Theft victim, consumer reporting agency or law enforcement).

B. Detection of Red Flags

In order to facilitate detection of the Red Flags identified in Attachment A, facility employees will take the following steps to obtain and verify the identity of the person.

1. New Patients/Accounts
 - a. Require identifying information (e.g., full name, date of birth, address, government-issued ID, insurance card, etc.).
 - b. When available, verify information with insurance company's information.
 - c. Verify the information with the consumer report (only when available).
2. Existing Accounts
 - a. Verify validity of requests for changes of billing address.
 - b. Verify identification of patients before giving out any personal information.

C. Preventing and Mitigating Identity Theft

	Information Security Policy	No.	COMP-Sec 4.1.3	
	Title:	Page:	5 of 6	
	IDENTITY THEFT PREVENTION PROGRAM (RED FLAG RULE)	Effective Date:	05-01-2009	
		Retires Policy Dated:		
		Previous Versions Dated:		

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 (Attachment A).

D. Program Administration

The Task Force is responsible for developing, implementing, administering and updating the Program. The Task Force will be responsible for developing a training program for staff identified by the Task Force as responsible for or having a role in implementing the Program.

E. Service Provider Arrangements

Tenet 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.

F. Updating of Program


The Task Force 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.

G. Enforcement

All employees whose responsibilities are affected by this policy are expected to be familiar with the basic procedures and responsibilities created by this policy. Employees who fail to comply with this policy may be subject to appropriate disciplinary action in accordance with all applicable policies and procedures, up to and including termination. Such disciplinary action may also include modification of compensation, including any merit or discretionary compensation awards.

VI. REFERENCES:

- Identity Theft Red Flags (Final Rule); 16 CFR Part 681 (November 9, 2007)
- Business Office Procedure Manual #05.01.10 Identity Theft/Theft of Services
- Human Resources Policy HR 116 No Retaliation
- Information Security Policy #1.0.0 Corporate Information Security Policy
- Information Security Policy #2.0.0 Record Processing Policy
- Information Security Policy #2.1.0 Information Classification Standard
- Information Security Policy #4.1.1 Incident Response Procedure
- Patient Access Policy - Validating Patient Identity

	Information Security Policy	No.	COMP-Sec 4.1.3	
	Title:	Page:	6 of 6	
	IDENTITY THEFT PREVENTION PROGRAM (RED FLAG RULE)	Effective Date:	05-01-2009	
		Retires Policy Dated:		
		Previous Versions Dated:		

VII. ATTACHMENTS:

- Attachment A: Relevant Identity Theft Red Flags Mitigation and Resolution Procedures
- Attachment B: Governing Board/Board of Directors Approval Form

Relevant Identity Theft Red Flags Mitigation and Resolution Guidelines

IDENTITY THEFT RED FLAG	PREVENTION/MITIGATION PROCEDURE	RESOLUTION OF RED FLAG
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 previously provided by the patient. For example, the date of birth provided is 9/22/1964 and the date of birth on file is 9/2/1964.	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.
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).	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.	Depending on the inconsistency and review of previous file, either delay or do not open a new covered account, or terminate services. If the results of the

Relevant Identity Theft Red Flags Mitigation and Resolution Guidelines

IDENTITY THEFT RED FLAG	PREVENTION/MITIGATION PROCEDURE	RESOLUTION OF RED FLAG
		investigation do not indicate fraud, all contact and identifying information is re-verified with patient.
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.	Investigate complaint, interview individuals as appropriate.	Terminate treatment/credit until identity has been accurately resolved; refuse to continue attempting to collect on the account until identity has been resolved. Notify law enforcement as appropriate. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.
Complaint/inquiry from a patient about information added to a credit report by a health care provider or insurer	Investigate complaint, interview individuals as appropriate.	Terminate treatment/credit until identity has been accurately resolved; refuse to continue attempting to collect on the account until identity has been resolved. Notify law enforcement as appropriate. If the results of the investigation do not indicate fraud, all contact and identifying information is re-verified with patient.
Complaint or question from a patient about the receipt of a collection notice from a bill collector.	Investigate complaint, interview individuals as appropriate.	Terminate treatment/credit until identity has been accurately resolved; refuse to continue attempting to collect on the account until identity has been resolved. Notify law enforcement as

Relevant Identity Theft Red Flags Mitigation and Resolution Guidelines

IDENTITY THEFT RED FLAG	PREVENTION/MITIGATION PROCEDURE	RESOLUTION OF RED FLAG
		<p>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 patient, 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> <p>If the results of the investigation do not indicate</p>

Relevant Identity Theft Red Flags Mitigation and Resolution Guidelines

IDENTITY THEFT RED FLAG	PREVENTION/MITIGATION PROCEDURE	RESOLUTION OF RED FLAG
		fraud, all contact and identifying information is re-verified with patient.
<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. 	Investigate complaint, interview individuals as appropriate	<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>

Governing Board/Board of Directors Identity Theft Prevention Program Approval

Identity Theft Prevention Program

This program has been designed to facilitate compliance with the Federal Trade Commission’s (FTC) Identity Theft Red Flag Rule. The rule requires “creditors” (including hospitals) to develop an “Identity Theft Prevention Program” to detect, prevent, and mitigate identity theft.

The program, set forth in the attached Information Security Policy, consists of methods to detect behaviors that indicate fraudulent activity, procedures to prevent the establishment of false accounts, procedures to ensure existing accounts are not being manipulated, and procedures to respond to identity theft.

All Tenet facilities are required to adopt an Identity Theft Prevention Program no later than May 1, 2009. Relevant employees and contractors will be trained prior to the compliance date.

A report will be submitted to the Governing Board on an annual basis to update the Board regarding the effectiveness of the Program, a summary of any identity theft incidents, the hospital’s response to the incident, and recommendations for substantial changes to the program, if any.

Identity Theft Prevention Program Review and Approval

This plan has been reviewed and adopted by the [Facility Name] [Governing Board/Board of Directors/Committee of the Board (choose one)]. Appropriate employees have been trained on the contents and procedures of this Identity Theft Prevention Program.

Signatures:

1. _____ Printed Name	_____ Signature	_____ Date
2. _____ Printed Name	_____ Signature	_____ Date
3. _____ Printed Name	_____ Signature	_____ Date
4. _____ Printed Name	_____ Signature	_____ Date
5. _____ Printed Name	_____ Signature	_____ Date
6. _____ Printed Name	_____ Signature	_____ Date

Relevant Identity Theft Red Flags Mitigation and Resolution Guidelines

For Facilities Without a Governing Board or Board of Directors:

This plan has been reviewed and adopted by:

Printed Name of Tenet Facility Senior
Management Member

Position

Signature

Date