IDENTITY THEFT PROTECTION GUIDELINES

A. Identity Theft Prevention

All employees and contractors are expected to report potential Identity Theft immediately upon discovery or notification of the same. Reports should be made to Privacy and Security Compliance Officer, or designee. If reports are made to a supervisor or department director, that individual is expected to immediately forward the report to the Privacy and Security Compliance Officer.

B. Identity Theft Identification (Red Flags)

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).

C. Detection of Red Flags

In order to facilitate detection of the Red Flags, Tenet 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.

D. 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 Identity Theft Red Flags Mitigation and Resolution Table.

IDENTITY THEFT RED FLAGS MITIGATION AND RESOLUTION TABLE

IDENTITY THEFT PROTECTION GUIDELINES

IDENTITY THEFT RED FLAG	PREVENTION/ MITIGATION PROCEDURE	RESOLUTION OF RED FLAG
Documents provided for identification appear to have been altered/forged or 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. Patient Access will notify the affected insurance carrier or payor as necessary.
Mail sent to the patient is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the patient's covered account.	Skip-tracing procedures are used to find the patient's current mailing address.	Patient is located and contact information is updated.
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).	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 records, either delay or do not open a new covered account, or terminate services. If the results of the investigation do not indicate identity theft, all contact and identifying information is re-verified with patient.

IDENTITY THEFT PROTECTION GUIDELINES

IDENTITY THEFT RED FLAGS MITIGATION AND RESOLUTION TABLE		
IDENTITY THEFT RED FLAG	**PREVENTION/ MITIGATION PROCEDURE**	**RESOLUTION OF RED FLAG**
Complaint/inquiry from a patient about information added to a credit report by a health care provider or insurer; Complaint or question from a patient about the receipt of a collection notice from a bill collector; or Complaint/inquiry from an individual based on receipt of: • bill for another individual • bill for a product or service that the patient denies receiving • bill from a health care provider that the patient never patronized • notice of insurance benefits (or Explanation of Benefits) for health services never received.	All reported incidents/claims of identity theft or billing errors from patients or other external sources are first referred to Patient Access for review of the charges by date of service to determine whether or not a billing error has occurred. Terminate treatment/credit until identity has been accurately resolved and stop collection attempts on the account.	If the results of the investigation do not indicate identity theft or a registration/billing error, all contact and identifying information is re- verified with patient. Patient Access and Accounts Payable will process the claim(s) for payment for services rendered using the patient and guarantor information collected at the time of registration. Health Information Management will make no change to the medical record for this patient. If the results of the investigation indicate identity theft or a registration/billing error Patient Access will contact Health Information Management to have the medical records reviewed for accuracy and corrected, if applicable. Patient Access will work with Accounts Payable to adjust the billing information so that the affected patient is not charged for the services and/or collection efforts are stopped. Patient Access will notify the affected insurance carrier or payor for the affected patient, if necessary. If the results of the investigation indicate identity theft the Privacy and Security Compliance Officer will work with law enforcement and determine reporting obligations, as necessary.

IDENTITY THEFT PROTECTION GUIDELINES

IDENTITY THEFT RED FLAGS MITIGATION AND RESOLUTION TABLE		
IDENTITY THEFT RED FLAG	**PREVENTION/ MITIGATION PROCEDURE**	**RESOLUTION OF RED FLAG**
Entity 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; or Personal identifying information provided by the patient is associated with known fraudulent activity as indicated by internal or third- party sources used by the Entity. For example: • 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.	All reported incidents/claims of identity theft from patients or other external sources are first referred to Patient Access for review of the charges by date of service to determine whether or not a billing error has occurred. Terminate treatment/credit until identity has been accurately resolved and stop collection attempts on the account. Request copies of applicable police report, fraud affidavit, FTC complaint, or other applicable report from third-party. If not previously completed by patient, recommend filing a police report, FTC consumer identity theft complaint, and notifying their health insurance carrier, if applicable.	If the results of the investigation do not indicate identity theft or a registration/billing error, all contact and identifying information is re- verified with patient. Patient Access and Accounts Payable will process the claim(s) for payment for services rendered using the patient and guarantor information collected at the time of registration. Health Information Management will make no change to the medical record for this patient. If the results of the investigation indicate identity theft or a registration/billing error Patient Access will contact Health Information Management to have the medical records reviewed for accuracy and corrected, if applicable. Patient Access will work with Accounts Payable to adjust the billing information so that the affected patient is not charged for the services and/or collection efforts are stopped. Patient Access will notify the affected insurance carrier or payor for the affected patient, if necessary. If the results of the investigation indicate identity theft the Privacy and Security Compliance Officer will work with law enforcement and determine reporting obligations, as necessary.