Policy Name: Identity Theft Prevention Program	
Owner (Title, Committee, or Council): Texas Health Chief Compliance Officer	**Effective Date:** 03/06/2017
Approved By: Texas Health Board of Trustees	**Last Reviewed Date:** 03/06/2017
Page 1 of 13	

1.0 Scope:

1.1 Applicable Entities:
This policy applies to Texas Health Resources and its member entities and excludes the Texas Health joint venture entities.

1.2 Applicable Departments:
This policy applies to all Texas Health departments.

2.0 Purpose:

2.1 To establish a written Identity Theft Prevention Program pursuant to the provisions of Section 114 of the Fair and Accurate Credit Transactions Act of 2003 and the corresponding amendments to the Fair Credit Reporting Act.

3.0 Policy Statement(s):

3.1 Texas Health Resources (Texas Health) will implement and maintain a written Identity Theft Prevention Program to detect and respond to potential red flags of identity theft, with an objective of mitigating the risk of identity theft in connection with a Covered Account and limiting damage to the victim and to Texas Health.

4.0 Policy Guidance:

4.1 The Texas Health Identity Theft Prevention Program is included in this policy as Attachment A.

5.0 Definitions:

5.1 Account - An account is a continuing relationship established by an individual or entity to obtain a product or service for personal, family, household or business purposes and includes extensions of credit as well as deposit accounts.

5.2 Covered Account - A Covered Account is one that Texas Health offers or maintains:

5.2.1 That is primarily for personal, family, or household purposes and designed to permit multiple payments or transactions (such as a payment plan); or

5.2.2 Where there is a reasonably foreseeable risk to the customer or to Texas Health from identity theft.

5.3 Identity Theft - A fraud committed or attempted using the identifying information of another person without authority. Identifying information means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, such as:

5.3.1 Name, social security number, date of birth, driver's license or state or government issued identification number, alien registration number, passport number, employer or taxpayer identification number, or insurance card.

5.3.2 Unique biometric data, such as fingerprint, voice print, retinal or iris image

5.3.3 Unique electronic identification number, address, or routing code

5.3.4 Telecommunication identifying information or access device

5.4 Red Flag - A pattern, practice, or specific activity that indicates the possible risk of identity theft.

5.5 Social Engineering - The attempt to manipulate or trick someone, such as a Texas Health employee, into providing the personal or financial information of another person, such as a patient or customer, to someone who is not authorized to receive such information. A social engineer uses human interaction (social skills) as a tool to obtain information. The social engineer could pose as a Texas Health employee.

5.6 Pretext Calling - A practice of persuading someone to provide their personal information under false pretenses. A pretext caller may have limited information, such as customer's name, address, or SSN, and may pose as the customer (or an employee) in order to convince Texas Health employees to divulge confidential information.

6.0 Responsible Parties:

6.1 Texas Health Board of Trustees

6.1.1 Approving the initial program (Board of Trustees).

6.2 Texas Health Audit and Compliance Committee of the Board of Trustees

6.2.1 Oversight of the Program- delegated by the Texas Health Board of Trustees.

6.2.2 Receiving reports at least annually from the Texas Health Chief Compliance Officer.

6.2.3 Approval of material modifications to the Program.

6.3 Texas Health Chief Compliance Officer

6.3.1 Day-to-day oversight and operation of the Program.

6.3.2 Reports to management and the Texas Health Boards of Trustees.

6.4 All Texas Health Employees

6.4.1 Adhere to the program and report any suspicious activity to the entity compliance officer and/or the Texas Health Chief Compliance Officer.

7.0 External References:

Not Applicable

8.0 Related Documentation and/or Attachments:

8.1 Allegation of Identity Theft Involving Fraudulent Access to Healthcare Services (Business Office Procedure).

8.2 Amending Health Information Form (Forms are located on My THR Connection. Select Resources, HIPAA Privacy, Privacy Forms and Amendment Request).

8.3 Suspected Identity Theft Report Form

8.4 Texas Health Identity Theft Affidavit

8.5 Anti-Fraud Program - THR System Policy

8.6 Background Check - THR System Policy

8.7 Electronic Communications Acceptable Use - THR System Policy

8.8 Faxing Health Information - THR System Policy

8.9 Identity Theft Risk Assessment

8.10 Information Security Risk Management - THR System Policy

8.11 Section 114 of the Fair and Accurate Credit Transactions Act Policy

9.0 Required Statements

Not Applicable

Attachment A

TEXAS HEALTH
Identity Theft Prevention Program

OVERVIEW:

The Identity Theft Prevention Program (Program) has been developed pursuant to the provisions of Section 114 of the Fair and Accurate Credit Transactions Act of 2003 and the corresponding amendments to the Fair Credit Reporting Act. This Program applies to Texas Health and all of its wholly owned or wholly controlled affiliates. The Program describes how to detect and respond to potential red flags of identity theft, with an objective of mitigating the risk of identity theft in connection with a Covered Account and limiting damage to the victim and to Texas Health.

AREAS OF RESPONSIBILITY:

The Texas Health Board of Trustees, management, and staff are responsible for implementing and maintaining this written Identity Theft Prevention Program. The Board of Trustees is responsible for approving the initial Program. The Texas Health Audit and Compliance Committee of the Board of Trustees is responsible for:

- Oversight of the Program
- Receiving reports at least annually from the Texas Health Chief Compliance Officer, and
- Approval of material modifications to the Program

The Board of Trustees has designated the Texas Health Chief Compliance Officer with the responsibility for oversight of the development, implementation, and administration of the Texas Health Identity Theft Prevention Program, including recommending material changes to the program as needed from time-to-time.

Individual entity identity theft procedures may supplement this Program with specific processes for detecting and responding to red flags of Identity. It is the responsibility of entity management and staff to identify potential red flags of identity theft and respond according to this policy. Entity management and staff should be watchful for other red flags not specifically addressed in this policy and should inform the Texas Health Chief Compliance Officer or the applicable Entity Compliance Officer, as appropriate, for review and follow-up.

Anyone observing, hearing about or otherwise suspecting an activity that appears to be identity theft must immediately report the activity to his/her supervisor. The employee or his/her supervisor must also contact the Texas Health Chief Compliance Officer or the Entity Compliance Officer (who will co-ordinate with the Texas Health Chief Compliance Officer) immediately in accordance with Texas Health policy. The Texas Health *Suspected Identity Theft Report Form* should be used to report all known facts surrounding the suspicious activity to the Texas Health Chief Compliance Officer or the Entity Compliance Officer.

The Texas Health Chief Compliance Officer, with assistance as needed from the applicable Entity Compliance Officer, Texas Health Legal Services, applicable Entity Privacy and Information Security Officers, is responsible to review, process and investigate reports of suspected identity theft. All reports of suspected identity theft will be tracked and documented in the Texas Health electronic compliance case tracking system.

In addition, the Texas Health Chief Compliance Officer will:

- Identify trends in terms of fraud, loss to Texas Health, identity theft, and suspicious activity
- Determine necessary updates to Texas Health's Identity Theft Prevention Program
- Identify efficiencies that might be gained through coordination between Texas Health System efforts and Entity efforts in the detection and prevention of identity theft.

DEFINITIONS:

Account - An account is a continuing relationship established by an individual or entity to obtain a product or service for personal, family, household or business purposes and includes extensions of credit as well as deposit accounts.

Covered Account - A Covered Account is one that Texas Health offers or maintains:

- That is primarily for personal, family, or household purposes and designed to permit multiple payments or transactions (such as a payment plan); *or*
- Where there is a reasonably foreseeable risk to the customer or to Texas Health from identity theft.

Identity Theft – A fraud committed or attempted using the identifying information of another person without authority. Identifying information means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, such as:

- Name, social security number, date of birth, driver's license or state or government issued identification number, alien registration number, passport number, employer or taxpayer identification number, or insurance card.
- Unique biometric data, such as fingerprint, voice print, retinal or iris image
- Unique electronic identification number, address, or routing code
- Telecommunication identifying information or access device

Red Flag – A pattern, practice, or specific activity that indicates the possible risk of identity theft.

Social Engineering - The attempt to manipulate or trick someone, such as a Texas Health employee, into providing the personal or financial information of another person, such as a patient or customer, to someone who is not authorized to receive such information. A social engineer uses human interaction (social skills) as a tool to obtain information. The social engineer could pose as a Texas Health employee.

Pretext Calling **-** A practice of persuading someone to provide their personal information under false pretenses. A pretext caller may have limited information, such as customer's name, address, or SSN, and may pose as the customer (or an employee) in order to convince Texas Health employees to divulge confidential information.

RISK ASSESSMENT AND IDENTIFIED COVERED ACCOUNTS:

Texas Health has performed an identity theft assessment and identified Covered Accounts to include:

- Patient billing records for healthcare services

THE PROGRAM:

Texas Health's written Program is designed to detect, prevent, respond and mitigate identity theft in connection with opening a Covered Account or any existing Covered Account. The Program includes the following:

- Identification of Covered Accounts, taking into consideration methods used to open and access accounts, previous experiences with identity theft, and relevant red flags,
- Identification of relevant red flags to prevent and mitigate identity theft,
- Training for appropriate staff,
- Appropriate oversight of service providers that perform activities in connection with Covered Accounts,
- Periodic review of the effectiveness of the Program in accordance with a risk-based schedule,
- Periodic updates to the program to reflect changes in risks to patients and Texas Health from identity theft,
- Reporting to the Texas Health Audit and Compliance Committee of the Texas Health Board of Trustees at least annually on material matters related to the Program.

RED FLAGS—IDENTIFY, DETECT, AND RESPOND:

Texas Health's Identity Theft Red Flag Risk Assessment has identified red flags and risks of identity theft as appropriate to Texas Health's operations.

The Program includes red flags from the following categories:

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers,
- The presentation of suspicious documents,
- The presentation of suspicious personal identifying information,
- Unusual use/suspicious activity of covered account

- Notices from patients, customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with a Covered Account.

In general, whenever a red flag of identity theft cannot be resolved, information should not be released and transactions should not be processed.

SPECIFIC RED FLAGS TO WATCH FOR:

1. A complaint or question from a patient based on the patient's receipt of:
    a. A bill for another individual
    b. A bill for a product or service that the patient denies receiving
    c. A bill from a healthcare provider that the person never patronized, or
    d. A notice of insurance benefits (or explanation of benefits) for healthcare services never received
2. Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient.
3. A complaint or question from a patient about a collection notice from a bill collector.
4. A patient or insurance company report that coverage for legitimate hospital stay is denied because insurance benefits have been depleted or a lifetime cap has been reached.
5. A complaint or question from a patient about information added to a credit report by a healthcare provider or insurer.
6. A dispute of a bill by a patient who claims to be the victim of any type of identity theft.
7. A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance and there is reason to be suspicious of identity theft.
8. A notice or inquiry from an insurance fraud investigator for a private insurance company or a law enforcement agency.

GUIDELINES FOR PATIENT OR CUSTOMER IDENTIFICATION:

Operational procedures for Patient Access Services, Cashier Services, the Texas Health Business Office and other entity activities involved with patient accounts include identification policies/procedures that are designed to mitigate the risk of identity theft. The following are general guidelines for identification.

Photo and non-photo identification: In general, a government issued photo identification is preferred, with exceptions for non-photo identification in certain circumstances. Non-photo identification may also be used as a secondary source of identification.

By telephone: In general, before releasing information or taking any action related to an account where communication is via telephone, obtain at least three pieces of identifying information:

- The first piece of information that the patient/customer should provide is medical record number (if applicable), social security number or other account number such as insurance identifying number. Exceptions may be made where appropriate. For example, a new patient may not know their medical record number.
- The second and third identifiers may be taken from the list below of identifiers not typically found in someone's wallet or purse:
    - Date of service
    - Location of service
    - Type of service

If further verification is needed, a call back to the telephone number on record with Texas Health may be used.

Request By fax: Incoming fax requests should be verified. A patient or customer may obtain account information or action on an account via FAX, by providing a signed, written request accompanied by a copy of an unexpired government issued identification. Alternatively, a patient or customer's identity may be verified using the procedures to communicate by phone prior to sending the FAX. Whenever faxing Protected Health Information (PHI), precautions for the confidential and secure treatment of PHI must be taken according to the guidelines established in the Texas Health *Faxing Health Information* policy.

By e-mail: Verify the patient or customer's identification using the procedures for communicating with a customer by phone by obtaining three pieces of information. Any email containing personal health information must be encrypted in accordance with THR's *Information Security Electronic Communications Acceptable Use* policy.

SOCIAL ENGINEERING AND PRETEXT CALLING:

Identification policies/procedures are designed to mitigate the risk of attempted social engineering or pretext calling to obtain personal information.

These activities have one thing in common—an attempt to obtain personal information and use it for fraudulent purposes. Examples of red flags for social engineering and pretext calling include:

- A caller who cannot provide all relevant information
- A caller who professes to be an employee, but Caller ID does not agree with the employee's location
- A caller who is abusive and attempts to obtain information through intimidation
- A caller who tries to distract you by being overly friendly or engaging you in unrelated conversation to divert your attention or to circumvent Texas Health policy

NOTIFICATION TO THR OF SUSPECTED FRAUD OR IDENTITY THEFT:

IF a patient or customer/victim:

- Notifies Texas Health that someone has accessed healthcare services fraudulently by a person engaged in identity theft,
- Notifies Texas Health of unauthorized charges on a healthcare claim/bill,
- Requests information relating to fraudulent transactions resulting from identity theft, or
- Notifies Texas Health that they have been a victim of identity theft so Texas Health can be alert for further fraudulent access to healthcare services,

THEN:

- Positively identify the patient/customer according to identification procedures.
- Provide the patient/customer with a Texas Health Identity Theft Affidavit for completion and notify the Entity Compliance Officer or the Texas Health Chief Compliance Officer so an investigation can be done.
- Refer the patient/customer to Texas Health online resources and education regarding identify theft for additional protections they should pursue if their identity has been compromised. If the patient/customer prefers, mail this information regarding the additional protections to the patient/customer.
- If notification is directly from a law enforcement agency, notify Texas Chief Compliance Officer or the Entity Compliance Officer who will coordinate with Legal Services as needed.
- A "red flag" fraud alert will be placed on the patient account.
- The Texas Health Business Office will be notified to suspend any billing activity while an investigation is done.

INTERNAL ALERTS:

The Texas Health business office or applicable entity personnel may place an identity theft or "red flag" fraud alert on a patient's account. All employees are to follow any instructions on the alert and positively identify the patient/customer according to identification policies and procedures before providing information or processing a transaction on an account with such an alert. Contact the Texas Health Chief Compliance Officer or the Entity Compliance Officer with any questions regarding internal "red flag" fraud alerts placed on patient accounts.

CORRECTION OF MEDICAL RECORDS:

If an investigation confirms that a person is the victim of medical identity theft, all medical records will be corrected to purge all information entered as a result of the fraudulent activity. In some cases fraudulent information may have been added to a pre-existing medical record. In other cases, the contents of an entire record may refer only to the thief's health conditions, but under the victim's name and other identifying information. In either case, the fraudulent activity has the end result of having the potential to introduce errors into the file of the victim. If the thief is an unknown individual, the fraudulent information should be completely removed from the victim's medical record and held separately so there is no danger of mistreatment due to factual error in the file. The separate record is the "Jane Doe or John Doe" record. If the thief is a known individual, the victim's file can undergo the same kind of data extraction with the fraudulent information being purged to the correct individual's medical record. Also refer to

Texas Health's *Amending Health Information* policy. A checklist to correct patient registration, billing and/or medical record information is attached at the end of this policy.

INSIDER THREATS:

Identity theft can occur through insider methods that are difficult to detect. Any Texas Health employee suspecting fraudulent use of personal information by co-workers must immediately report the suspicion to their supervisor and to the Texas Health Chief Compliance Officer. Texas Health's *Background Check* policy must be adhered to. In addition, unsecured and unencrypted patient information on laptops, thumb drives and other portable devices can pose significant risk. All Texas Health Information Security policies must be adhered to at all times.

ENTITY SECURITY:

Any activity that necessitates contacting or communication with law enforcement should be coordinated with entity security personnel and legal counsel, as needed. Any issues or concerns that pose an immediate security threat to the safety of any patient or employee should be communicated directly to entity security.

TRAINING:

Training is provided for Program implementation and for new hires. Refresher training will be provided as needed.

OVERSIGHT OF SERVICE PROVIDERS:

The Program includes appropriate oversight of service providers that provide a service directly to Texas Health and perform activities in connection with a Covered Account. Appropriate oversight is determined on a risk based approach that considers, among other things, the type of service provided, the type of information the service provider has access to and the mitigating controls in place. Service providers may have their own Identity Theft Prevention Program to prevent identity theft.

Service providers may be required by contract to have appropriate policies and procedures in place to detect relevant red flags and either report the red flags to Texas Health or take appropriate steps to prevent or mitigate identity theft.

ADDRESS DISCREPANCY- OBLIGATIONS:

If any Texas Health activity includes using a nationwide credit report, the user must take appropriate action when a request for a credit report results in a Notice of Address Discrepancy. When the address supplied by the Texas Health user of the credit report differs substantially from the address in the credit bureau files, the bureau notifies the requestor of the existence of the address discrepancy. When the Texas Health user receives the notice the user must research the discrepancy to form a reasonable belief that the consumer report relates to the

consumer about whom the report was requested. The following are examples of steps to take:

- Compare information in the consumer report with information Texas Health has in its records previously used to identify the patient,
- Compare the information in the consumer report with information Texas Health maintains in its own records such as applications, change of address notices or other documentation,
- Verify the information in the consumer report with the consumer.

If the Texas Health credit report user has reasonably confirmed that the address provided in the consumer report is erroneous, the Texas Health user must furnish an address for the consumer to the consumer reporting agency that issued the Notice of Address Discrepancy when the Texas Health user:

a. Can form a reasonable belief that the consumer report relates to the consumer for whom the Texas Health user requested the report;
b. Establishes a continuing relationship with the consumer; and
c. Regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which the Notice was obtained.

Addresses may be reasonably confirmed as accurate by:

a. Verifying the address with the consumer,
b. Reviewing Texas Health records to verify the address of the consumer,
c. Verifying the address through third-party sources; or
d. Using other reasonable means.

PERIODIC REVIEWS:

Periodic internal review will be performed to determine the effectiveness of the Program.

UPDATES TO THE PROGRAM:

The Program will be reviewed at least annually. The risk assessment and Program will be updated as necessary to reflect changes in risks to patients based on such factors as:

- Texas Health's experiences with identity theft
- Changes in methods of identity theft
- Changes in methods to detect, prevent, and mitigate identity theft
- Changes in the types of accounts that Texas Health offers or methods to access those accounts, and
- Changes to Texas Health business arrangements, including mergers, acquisitions, and service provider arrangements.

Material changes to the Program will be approved by the Texas Health Audit and Compliance Committee of the Texas Health Board of Trustees.

REPORT TO THE Texas Health AUDIT AND COMPLIANCE COMMITTEE:

Texas Health Chief Compliance Officer will report to the Texas Health Audit and Compliance Committee of the Texas Health Board of Trustees no less than annually on material matters related to the Program, such as:

- the effectiveness of the policies and procedures in addressing the risk of identity theft in connection with new and existing accounts patient or customer accounts;
- service provider arrangements;
- significant incidents of identity theft and management's response; and
- material changes to the Program.

References:

Texas Health Identity Theft Risk Assessment

Texas Health Policy: Anti-Fraud Program Policy

Texas Health Business Office Procedure: *Allegation of Identity Theft Involving Fraudulent Access to Healthcare Services*

Texas Health Policy: *Background Check*

Texas Health Privacy Program Policies:

- *Amending Health Information (Forms are located on My THR Connection. Select Resources, HIPAA Privacy, Privacy Forms and Amendment Request)*
- *Electronic Communications and Acceptable Use*
- *Faxing Health Information*
- *Identity Verification for Health Information Disclosures*

Texas Health Information Security Program Policies