



Healing Hands. Caring Hearts.™

Elaine Anderson, CPA
SVP, Chief Compliance Officer
HFMA –Lone Star Chapter, Central
Texas Meeting
October, 16, 2009

Identity Theft Prevention Program: Compliance with “Red Flag Rules”

Prior to Red Flags Rules

- THR had an identity theft policy and process in place including:
 - How to identify and report potential ID Theft
 - An ID Theft Affidavit for use with patients alleging ID Theft
 - How to hold the patient billing account during investigation
 - Tools to assist the ID theft victim (credit watch, etc.)
 - Awareness training had been done with key areas such as business office

After Red Flag Rules



- Adopted more formalized and detailed program
- Strengthened/expanded education
- Clarified reporting chain and accountabilities
- Implemented better/more consistent tracking
- Implemented automated "Red Flag Alert" for patient accounts



Rule: Periodic Identification of Covered Accounts



- Conducted risk assessment
- Determined that patient accounts are "covered accounts"
- Also aware of "internal risk" that an employee or agent could misuse personal information of a non-patient (i.e. employee, physician, other contractor, etc.).



Rule: Written Plan



- Established steering committee to develop written plan in Sept. 2008
- Used the World Privacy Forum, September 2008 Whitepaper: *Red Flags and Address Discrepancy Requirements: Suggestions for Health Care Providers* as a significant resource in writing the plan
- Also reviewed “red flag” policy of a financial institution and other materials



Rule: Identify Red Flags



- Written plan includes description of categories of Red Flags
 - Notifications or warnings from consumer reporting agencies or service providers
 - Presentation of suspicious documents
 - Presentation of suspicious personal identifying information
 - Suspicious activity of a covered account
 - Notices from patients, law enforcement, etc;.



Specific Red Flags to Watch For







- Complaint or question from a patient
 - Bill for another
 - Bill for service not received
 - Bill from a provider never seen
 - Notice of insurance benefits for services not received
- Records inconsistent with treatment or medical history
- Complaint about collection notice
- Insurance denial due to benefits depleted or lifetime cap reached
- Complaint about credit report
- Dispute of bill by person claiming to be an ID theft victim
- Patient with insurance number, but no card
- Suspicious documents/lack of identifying information

Rule: Detect and Log/Report on Red Flags



- Complete the Texas Health Suspected Identity Theft Report form, located on the intranet under forms
- Discuss with supervisor
- Notify the Entity Compliance Officer or the Texas Health Chief Compliance Officer so incident can be logged into tracking system and an investigation can begin
- Compliance Officer places a "red flag" fraud alert on the patient account and billing is suspended pending outcome of the investigation

Suspected Identity Theft Report Form



TEXAS HEALTH RESOURCES
Suspected Identity Theft Report Form

Name of Person Completing Report: _____ Date: _____
Entity and department: _____ Phone: _____

Describe suspicious activity or "red flag" in detail:

Account or Medical Record Number, if known: _____

Potential Identity Theft Victim Information, if known:

(1) Full legal name:

(First) (Middle) (Last) (Jr., Sr. III, etc.)

(3) Date of birth _____
(month/day/year)

(4) Social security number _____

(5) Driver's license or identification card number and state _____




(6) Current address _____
City _____ State _____ Zip Code _____

(7) Daytime telephone number () _____

(8) Evening telephone number () _____

(Attach additional sheets or information as needed to provide all details)

Rule: Respond to Red Flags

- 
- 
- 
- 
- Obtain all information necessary to investigate from victim
 - Provide assistance to victim to mitigate harm
 - Investigation initiated to validate or disprove ID Theft allegation (Coordinated by compliance function)
 - "Red Flag Alert" placed on patient account in question

Information Needed to Investigate a Customer Identity Theft Allegation



- Notarized ID Theft Affidavit:
 - Full name of victim
 - Victim's personal and demographic information
 - Victim's Contact information
 - How fraud occurred (e.g. stolen wallet)
- Copy of Police Report
- Proof of victim's residency during the time the disputed bill occurred
- Copy of victim's valid government issued photo-identification card
- Any other information the victim can provide

Patient Account Red Flag Alert



- When a patient account is involved with suspected identity theft a red flag alert is placed on the patient's account by the Entity Compliance Officer.
- Employees Must follow the instructions on the red flag alert before:
 - providing information
 - registering the patient
 - processing a transaction on the accountAnd.....
- Contact supervisor immediately

What Will a Red Flag Alert Look Like?



RED FLAG ALERT - POSSIBLE MEDICAL IDENTITY THEFT

Current investigation in process. Positively identify this patient prior to: registration, releasing information or discussing details of the account. Contact supervisor.



Assisting the Victim and Taking Corrective Action



- If an investigation confirms that a person is the victim of medical identity theft, action is taken to assist the victim.
 - Medical records and hospital information systems are corrected to purge all information entered as a result of the fraudulent activity.
 - Other providers, such as Emergency Department Physicians involved in the care of the patient are notified.
 - The Business Office resolves account balances.
 - Removal of negative credit reported by Texas Health from the patient's credit report.
 - Notification to insurance company, if applicable
- A THR checklist is used to document all necessary steps/corrective actions



Rule: Update program



- Written program includes requirement that the program be periodically reviewed and updated
- Incidents are tracked and trended and will be taken into consideration in review and updates



Rule: Training



- New employee orientation includes basic ID Theft overview
- Focused ID Theft training provided for certain job functions
- Annual refresher training for all employees includes ID Theft awareness training
- Certain job functions also required to complete in-depth ID Theft *refresher* training in addition to basic awareness provided to all employees



Rule: 3rd Party Service Providers

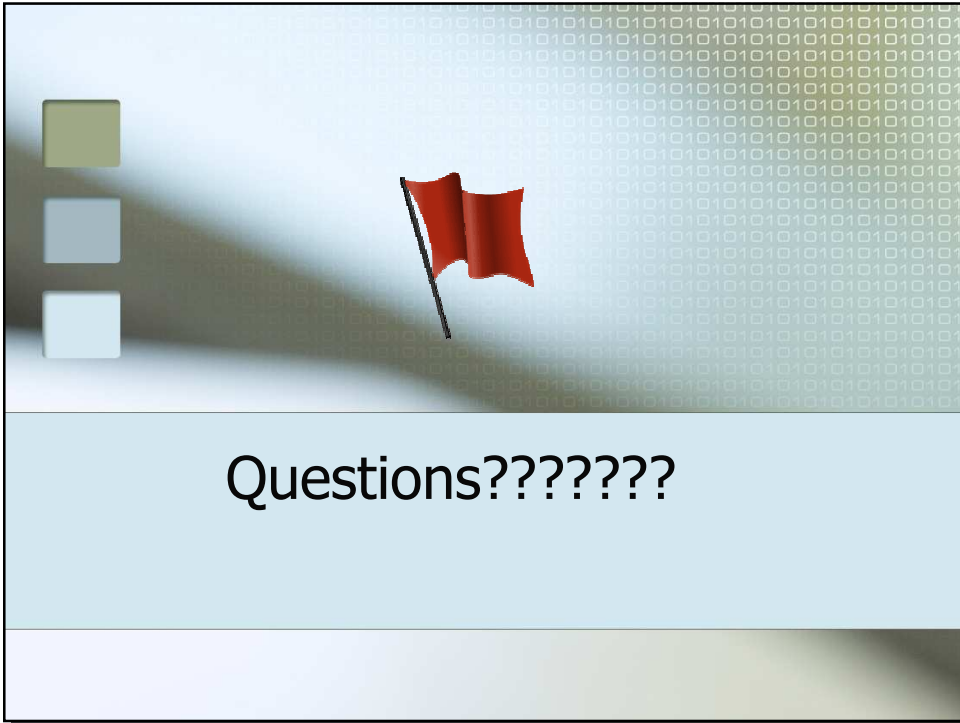


- All service providers with a business associate agreement will receive a BA amendment and written notice regarding their obligations under the THR ID Theft Program. Amendment covers both Red Flags provision and HITECH Act changes.
- BA agreement updated to include obligations under ID Theft Program for new service providers

Rule: Oversight



- Approved by the THR Board in October, 2008
- Program is under the oversight of the THR Chief Compliance Officer with reporting to the THR Audit & Compliance Board Committee
- Entity compliance officers are accountable at entity level
- Annual report provided to the THR Audit & Compliance Committee and THR Board.
- Each hospital board receives report from the entity compliance officer



Questions???????