Red Flags Identity Theft Prevention Program
The information contained in this module is maintained and reviewed annually by educators.

Efforts were made to present the following content in an accurate, clear, and concise manner while maintaining compliance with acceptable standards of care. Your comments and concerns are important to us.

Please do not hesitate to provide feedback or identify errors, omissions or deficiencies in the content or presentation of this important subject matter.

Contact: HSC Compliance Office
E-mail: Compliance@salud.unm.edu
Phone: 925-6053
Red Flags Identity Theft Prevention Program

Objectives

After completing this training, you will be able to:

- Understand identity theft and medical identity theft
- Understand the Red Flag Identity Theft Rule
- Identify potential indicators of Identity Theft
- Understand how a Red Flag is assigned
- Know the process when a Red Flag is set
- Understand how to report a suspected Red Flag or Identity Theft
What is identity theft?

- Identity theft occurs when one person fraudulently uses the identity of another, usually for the purposes of obtaining credit, benefits, or services. This can cause great financial harm to the victim.

- Medical identity theft is a special case of identity theft in which the identity of another is used fraudulently to obtain health care items or services. Not only do victims suffer financial harm, they may also receive improper care when incorrect information is entered into existing medical records because future providers may rely on the medical record when making care decisions.
The Red Flag Identity Theft Rule

In 2007 the Federal Trade Commission (FTC) and other banking regulatory agencies issued the Red Flag Identity Theft Rule. It is designed to protect consumers by standardizing the manner in which institutions respond to identity theft. Any institution that extends credit must have procedures in place to identify, detect and respond to specific activities that could indicate identity theft. UNM HSC and UNM HS Entities may offer “credit” in the form of payment plans to patients; therefore, we are obligated to comply with this regulation.

Reference: FTC Red Flags Rule 16 CFR 681.2
What is a Red Flag?

- In order to comply with the FTC’s Red Flag Identity Theft rule, the Red Flags Identity Theft Prevention Program procedure has been adopted.

- Under the Red Flag procedure, a Red Flag is two things:
  1. A sign that a person’s identity may have been compromised
  2. A pop-up alert in PowerChart used to indicate that an account has been, or may have been, compromised.
Signs of Identity Theft

In order to protect the identities of our patients, look out for signs of identity theft. There are four main categories of identity theft:

Suspicious documents, for example:

- Did the patient sign the correct name on the registration form?
- Do documents appear to be forged or altered?
- Is the information on the insurance card consistent with photo ID?

Suspicious personal identifying information, for example:

- Is this person’s age/gender/race/ethnicity consistent with previous visits?
- Is the information in the patient’s medical record consistent with the physical exam?
Red Flags Identity Theft Prevention Program

**Signs of Identity Theft (Continued)**

**Suspicious or unusual use of accounts**, for example:
- Was payment denied by insurance because the patient’s lifetime cap is met?

**Alerts from others**, for example:
- Has the patient reported to you that he or she was billed for items or services that he or she did not receive?
- Is the patient a victim of identity theft at other institutions?
- Has law enforcement alerted you to possible risk?
- Is there a Red Flag alert on the patient’s account?

Approximately one-quarter of HSC suspected red flag/identity theft matters have been the result of an error during patient registration or elsewhere during the admission process.
Accounts with Red Flag Alerts

The HSC Compliance Office is responsible for placing Red Flag alerts on patient accounts and coordinating investigation activities.

What are the steps?

- First, HSC Compliance becomes aware of possible identity theft, usually from Patient Financial Services, Health Information Management, or Registration Staff.
- Once HSC Compliance learns of potential identity theft, or risk of identity theft, HSC Compliance works with other departments to coordinate an investigation.
- If HSC Compliance determines that it is necessary to place a Red Flag Alert in order to protect account integrity, HSC Compliance places the Alert and notifies the patient in writing.
- Only HSC Compliance can place a Red Flag Alert on a patient account.
- If you see any of these signs of identity theft, or other suspicious behavior that you believe might indicate identity theft, report it to your supervisor. Your supervisor will report the incident to HSC Compliance and determine how best to proceed.
Red Flags Identity Theft Prevention Program

Registering a Patient with a Red Flag Alert

If a patient account has had a Red Flag Alert placed, a pop-up alert will display during the normal registration process in PowerChart. When that happens:

✓ The Registrar asks for photo ID, uses the script to explain why to the patient, and notifies his or her supervisor.

✓ If the patient presents valid photo ID:
  – Register the patient with the correct insurance information
  – Make a photo copy of the photo ID and label the copy with a double bar code sticker
  – Write “Red Flag” on the photo copy
  – Send the copy to Patient Billing and Collections Offices
Registering a Patient with a Red Flag Alert (Continued)

- If the patient does NOT present valid photo ID:
  - Register the patient with guarantor account Red Flag # 99997870
  - Notify a nurse or physician that the patient’s account has a Red Flag Alert and that the patient did not present valid photo ID.

*Make sure that the nurse or physician understands that the patient’s account is at a high risk for identity theft and because the patient’s identity could not be verified, there is a high risk that the information in the patient’s medical record is incorrect.*
Reporting a Red Flag or suspected Identity Theft

- All instances of known or suspected identity theft or compromised identity must be reported to HSC Compliance.

When you suspect identity theft or a patient has stated that his/her identity has been stolen:

- Gather as much information as possible to assist Compliance with the investigative process (names, telephone numbers, MRNs, FINs, etc.)
- Report the matter to your supervisor or manager
- Scan or copy all documentation gathered (e.g. Driver’s license provided by patient, insurance cards, etc.)
- Supervisor or manager will be responsible for reporting to HSC Compliance via secure e-mail (* secure * in the subject line)
- Assist Compliance Department with investigation as requested
- Compliance will determine whether it is necessary to place a red flag alert on the subject MRN
In this training, you have learned:

- Information about identity theft and medical identity theft
- The Red Flag rule as it relates to identity theft
- The potential indicators of identity theft
- How to report suspected identity theft
- The process that UNM Hospitals follows when a patient has a Red Flag alert