Introduction

- Fair and Accurate Transaction Act (FACTA)

- Congress – Federal Trade Commission and other
  Other agencies to develop regulation requiring “creditors” and “financial institutions” to address risk of identity theft.
Introduction

- November 9, 2007
  - FTC and other agencies issued regulations that require the detection, prevention and mitigation of identity theft – RED FLAGS RULE
- November 1, 2008 – Original Effective Date
- Postponed to May 1, 2009 and again until
- August 1, 2009.
Requirement of the Red Flag Rule

• Financial institutions and creditors with covered accounts must establish an identity theft prevention program to identify RED FLAGS and to prevent and mitigate identity theft.
FACTA’s definition of a creditor is extremely broad and includes all entities that regularly permit payments for goods and services. However, accepting credit cards as a form of payment does not, by itself, make an entity a creditor.
Covered Account

- Any other account that the financial institution or creditor offers or maintains for which there is a reasonable foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft.
Creditor

• UTMC is a creditor because...

• it regularly bills patients after the completion of services, including for the remainder of medical fees not reimbursed by insurance.

• it regularly sets up payment plans after services have been rendered.
The Red Flag Rule defines Identity Theft as:

- A pattern, practice, or specific activity that indicates the possible existence of identity theft.
What is Identity Theft?

- Occurs when someone uses another person’s identifying information without permission to commit fraud or other crimes
  - This information could include:
    - Name
    - SSN
    - Insurance Number
    - Credit Card Number

- **Potential Consequences**
  - False Diagnosis
  - Unsafe care or deadly care
  - Future denials of insurance coverage
What can employees do?

• Be alert and considerate of everyone by implementing:
  • Safeguards to prevent identity theft
  • Procedures to detect suspicious activities
  • Reporting procedures when suspected identify theft has occurred.
How to Prevent, Detect, and Report

• Create a program to **prevent, detect, and report** Identity Theft to reduce the harmful effects of Identity Theft such as:
  • A policy dedicated to identity theft
  • Education on Red Flag – Fraud Alerts
  • A Red Flag Committee
  • An Identity Theft Response Team for Investigations
Prevention

- **Always** use shredders for confidential/PHI information
- Keep passwords secure and **do not** share them
- Eliminate the use of SSN wherever it is possible

- 3364-15-12 Identity Theft Prevention, Detection, and Mitigation [http://www.utoledo.edu/policies](http://www.utoledo.edu/policies)
Detection

- Detecting Identity Theft Red Flags is dependant on awareness of suspicious activities common to the department where you work.
Be Proactive

• If you think of additional Identity Theft Red Flags common to your department share them with your supervisor to raise awareness for your department!
Reporting

- Identity Theft must be reported as soon as it is suspected!
  - Contact manager
  - Contact Campus Police

Do not delay emergency treatment
A patient may contact UTMC after being a victim of Identity Theft.

They may complete the Passport Program offered by the Federal Trade Commission.

This form is available at: http://www.ftc.gov/bcp/edu/microsites/idtheft/
Contact Information

• Contact your supervisor

• Contact the Compliance Office
  • Lynn Hutt Compliance/Privacy Officer
    419-383-6933
Examples of Red Flags

- **Suspicious Personal ID info**
  - Info presented inconsistent with external info
  - Info presented inconsistent with info on file
  - ID associated with known fraud activity or previous red flag
  - Duplicate ssn
  - Duplicate medicaid card
  - Duplicate address or telephone #
  - Incomplete info
  - Person unable to authenticate presented info

- **Suspicious Activity**
  - New or replacement request shortly following address change
  - Usage consistent with known fraud patterns
  - Unusual usage, inconsistent with normal patterns
  - Mail returned despite continued confirmation of address
  - Person complains about receiving a bill denying receipt of services
Examples Cont.

- **Suspicious Medical Information**
  - Person presents medical background inconsistent with existing medical record
  - Person unaware of basic medical background
  - Medical record inconsistent with physical examination of patients account of medical history
  - Person’s insurance company report that coverage for legitimate hospital stay is denied because benefits have been depleted
  - Person denies info provided in medical record
  - Lab (blood work, type etc) inconsistent with info in medical record
  - Person refuses to provide insurance card

- **Suspicious Documentation**
  - Altered/forged ID
  - Inconsistent photo/description
  - ID info doesn’t match what is on file
  - Altered/forged application
WHAT IS A RED FLAG?

- RED FLAG A
- RED FLAG B
- RED FLAG C
- RED FLAG D
- RED FLAG E
Resources

- Federal Trade Commission-Identity Theft
  - http://www.ftc.gov/bcp/edu/microsites/idtheft/

- Attorney Generals Office-Identity Theft
  - http://www.ag.state.oh.us/victim/idtheft/index.asp
RED FLAG

THANK YOU!