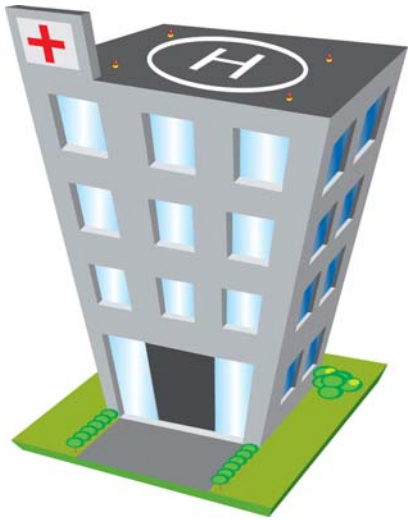




# Update on Red Flags Rule

## Applicability to Health Care Providers



Rebecca L. Williams, RN, JD  
Partner  
Co-Chair, HIT/HIPAA Practice  
Davis Wright Tremaine LLP  
Seattle, WA  
[beckywilliams@dwt.com](mailto:beckywilliams@dwt.com)



# Focus of Red Flags Rule: Identity Theft



- Fraud committed or attempted by using identifying information of another person (individual or entity) without authority
- Identifying information:
  - Name, SSN, EIN, DOB, government issued identification number (drivers license, passport, etc.)
  - Unique biometric data (fingerprints, voice print, retina image, etc.)
  - Unique electronic identification number, address, or routing code
  - Telecommunication identifying information or access device

# A Twist in Health Care: Medical Identity Theft

- Individual's name and personal identifiers are used by another to fraudulently receive medical services and goods (or to commit billing fraud)
  - individual attack
  - mass attack
- Can corrupt medical and insurance records
- Fast(est) growing form of identity theft
- May be underreported



# History of the Red Flags Rule: A Long and Winding Road

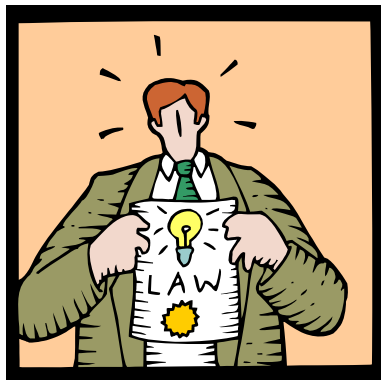
The Fair Credit Reporting Act (FCRA) was enacted in 1970



In 2003, Congress passed the Fair and Accurate Credit Transactions Act (FACTA), which amended the FCRA



FACTA included a directive to create identity theft regulations. The Red Flags Rule is the result -- Jointly issued by the FTC and five other federal agencies



# History of the Red Flags Rule: A Long and Winding Road of FTC Compliance Dates

Nov. 1, 2008  
Original  
Compliance  
Date

Aug. 1, 2009  
Delayed Compliance  
Date

Nov. 1, 2009  
Delayed  
Compliance  
Date



May 1, 2009  
Delayed  
Compliance  
Date

Oct. 2009  
House Bill

Latest  
Compliance  
Date  
**June 1, 2010**



# To Whom do the Red Flags Rule Apply?



Entities Subject  
to the  
Red Flags Rule



## Creditors

- “Any entity that regularly extends, renews, or continues credit.”
- Credit is “the right granted by a creditor to a debtor to **defer payment** of debt or ... to purchase ... services and defer payment therefor.”

Subject to FCRA  
Enforcement  
FCRA not limited to  
for-profit entities

## With Covered Accounts

Accounts for family/  
personal purposes, or  
with risk of  
identity theft

# Application of Red Flags Rule to Health Care Providers

- FTC has announce that health care providers could be considered “creditors”
- Preamble makes passing reference to medical identity theft, but does not explicitly identify health care providers as creditors
- FTC publications include health care providers



# But Wait... Does the Red Flags Rule Apply to Health Care Professionals?

- August 2009 – American Bar Association filed a complaint to block the FTC from applying Red Flags Rule to attorneys. ABA claimed:
  - FTC exceeded powers – misinterpreted FCRA
  - Since a fee cannot be charged until a service is rendered, the fact a service precedes a bill ≠ credit.
  - No rational connection ↔ practice of law and identity theft
- October 2009 – ABA wins
- Appeal . . . Deadline fast approaching
- January 27, 2010 – Joint request by AMA, AOA, ADA, AVMA that FTC to not apply Red Flags Rule to health care professionals





# If Red Flags Rule Does Apply

- Periodic identification of “covered accounts”
- Establishment of an Identity Theft Prevention Program
  - Designed to detect, prevent, and mitigate identity theft in connection with covered accounts
  - Appropriate to the size and complexity of the organization
- Ongoing administrative responsibilities



# Requirements of a Red Flag Program



- **Identify covered accounts**

- Consumer accounts, primarily for personal, family, or household purposes, designed to permit multiple payments or transactions
  - No risk determination needed
- Any other accounts that present a reasonably foreseeable risk of identity theft (including financial, operational, compliance, reputation, or litigation risk
  - Foreseeable risk
- Look at existing and new accounts



# Requirements of a Red Flag Program



- **Identify red flags**

- Red flag: pattern, practice, or specific activity that indicates the possible existence of identity theft
- Process
  - Consider the type of accounts offered and maintained
  - Consider the methods to open and access covered accounts
  - Review previous experiences with identity theft, including instances of medical identity theft

# Sources of Red Flags



- Incidents of identity theft
- Identity theft methodology – and changes
  - Alert notification, credit “freeze” or warning from a consumer reporting agency or service provider
  - Suspicious document being presented (such as seeming forgery, inconsistent physical description/photo, inconsistent information)
  - Suspicious personal identifying information being presented
  - Inconsistencies with other sources of information
  - Action consistent with known fraudulent activity
  - Failure to provide all required personal information
  - Unusual use of or suspicious activity related to a covered account
  - Notice from consumers, victims, law enforcement, others



# Requirements of a Red Flag Program



- **Detect red flags.** Develop processes to:
  - Authenticate patients/customers (e.g., requiring that patients present ID but beware EMTALA)
  - Monitor transactions
  - Verify change-of-address requests

# Requirements of a Red Flag Program

- **Respond to red flags.** Prevent and mitigate identity theft:
  - “Appropriate responses” include:
    - Monitoring covered accounts
    - Contacting patients
    - Changing account passwords, security codes and devices
    - Notifying law enforcement
    - Not attempting to collect on account or sell to debt collector
  - May be appropriate to take no action



# Requirements of a Red Flag Program

- **Ensure program is regularly updated**
  - To prevent reoccurrence of actual experience with identity theft
  - To reflect changes to business structure
  - To respond to changes in the methods of identity theft and methods to detect identity theft



# Requirements of Red Flag Program

- **Administrative responsibilities**

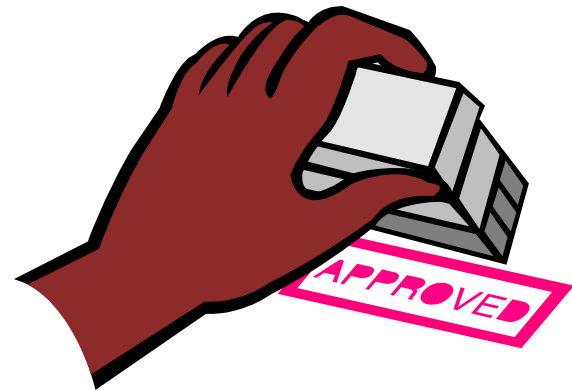
- Document program
  - Reasonable policies and procedures
  - May want to incorporate Red Flags program into an existing program
- Train staff
- Oversight of service provider arrangements
  - Ensure service provider has protections to detect, prevent, and mitigate risk of identity theft
- Annual reports by staff
  - Effectiveness
  - Significant incidents and responses
  - Service provider arrangements
  - Recommendations





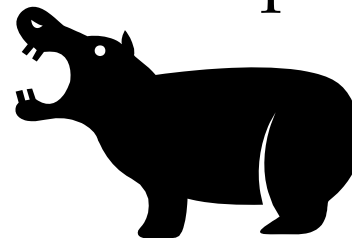
# Requirements of Red Flag Program

- **Board and Senior Leadership Involvement**
  - Get initial approval from the board of directors or appropriate board committee
  - Continued oversight of the Program by the board, a board committee, or designated senior management



# HIPAA and Red Flags Rule

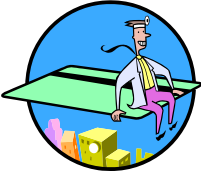
- HIPAA privacy and security requirements help keep personal information from falling into the hands of identity thieves
- Red Flags Rule goes another step
  - If identity thieves obtain personal information, they typically try to get goods and services without paying
  - Red Flags Rule seeks to reduce the damage identity thieves can inflict on the providers and the patients



# Similarities between HIPAA/HITECH & Red Flags Rule

## HIPAA/HITECH

## Red Flags Rule

|  |  |
|--|--|
| <p>Security standards focused primarily on an entity's performance of "<b>risk analysis</b>" and "<b>risk management</b>"</p>  | <p>Provide a "<b>risk-based</b>, non-prescriptive approach"</p>  |
| <p>"<b>Flexibility</b> of approach," allowing covered entities to use "any security measures that...reasonably and appropriately implement the [HIPAA security] standards"</p> | <p>Provide for "<b>flexibility</b>...to adapt to rapidly changing risks of identity theft"</p>  |
| <p>Program should take into account the "<b>size, complexity</b>, and capabilities of the covered entity"</p>  | <p>Program should "be appropriate to the <b>size</b> and <b>complexity</b> of the financial institution or creditor and the nature and scope of its activities"</p>                |





# HIPAA/HITECH & Red Flags Rule

## HIPAA/HITECH

## Red Flags Rule

|  |   |
|--|---|
| Focus: Protected health information (includes demographic information)                         | Focus: Covered accounts (including identifying information) |
| Protect against improper uses and disclosures (and preserve integrity and availability of PHI) | Protect against identity theft                              |
| Mitigation   | Mitigation  |
| Breach notification  | Response to red flags                                       |
| Business associate (in connection with PHI)  | Service providers (in connection with covered accounts)     |



# Questions?

Rebecca L. Williams, RN, JD  
Partner  
Co-Chair, HIT/HIPAA Practice  
Davis Wright Tremaine LLP  
Seattle, WA  
[beckywilliams@dwt.com](mailto:beckywilliams@dwt.com)

