Red Flags Rule

Agenda:

- What is the Red Flags Rule?
- Four Steps to Compliance
  - Identify Red Flags
  - Detect Red Flags
  - Prevent and Mitigate Identity Theft
  - Update the Program
- Resources
- Service Providers
What is the Red Flags Rule?
What is the Red Flags Rule?

The Federal Trade Commission (FTC), along with federal bank regulators and the National Credit Union Administration, adopted regulations in 2008 implementing the Federal law commonly known as the Red Flags Rule.
What is the Red Flags Rule?

“In 2008, the World Privacy Forum found that the number of Americans identifying themselves in government documents as victims of *medical* identity theft had tripled in just 4 years to more than a quarter-million in 2005.” – MSNBC.com

The FTC estimates that as many as nine million Americans have their identity stolen each year.
What is the Red Flags Rule?

Victims of *medical* identity theft face possible complications when their medical history is confused with that of the thief, including:

- Erroneous medical bills
- Loss of insurance benefits
- Unnecessary medical procedures
- Inability to obtain health, life, or disability insurance
- Harm caused when treatment is based on incorrect information
What is the Red Flags Rule?

In Seattle, Washington, the family of baby “Andrew” received a collection notice for unpaid bills for treatment of Andrew’s work-related injury.

In Huntington Beach, California, a woman has been accused of stealing another woman’s identity to trade in the thief’s breast implants for new ones and for liposuction - $12,000 worth of services.
What is the Red Flags Rule?

Identity theft not only costs consumers heartache, time and money – it impacts businesses whose services have been stolen.
What is the Red Flags Rule?

The Red Flags Rule requires creditors that offer/maintain covered accounts to adopt a written identity theft prevention program to:

- **Detect** warning signs of identity theft (Red Flags) in day-to-day operations,
- **Take steps to Prevent** the crime, and
- **Mitigate** (alleviate) the damage it causes.
What is the Red Flags Rule?

Important Definitions

If a health care provider allows for payment on medical services provided to a patient after those services were provided and/or over a period of extended payments, the health care provider is considered a “creditor.”
What is the Red Flags Rule?

Important Definitions

A "covered account" is defined as "an account primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, or any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the creditor from identity theft."
What is the Red Flags Rule?

Important Definitions

USC School of Medicine University Specialty Clinics® meets the definition of a “creditor” and offers/maintains “covered accounts;” therefore, in compliance with the law, we have an Identity Theft Prevention and Detection Program (effective May 1, 2009).
What is the Red Flags Rule?

Important Definitions

An effective identity theft prevention program equips employees to recognize and respond to Red Flags so that identity theft may be prevented or mitigated.

A “Red Flag” is defined as “a pattern, practice or specific activity involving a patient that indicates the possible existence of identity theft.”
What is the Red Flags Rule?

Health care providers are most likely to detect Red Flags during the process of:

- Registering/authenticating new and current patients
- Submitting claims for payment and billing patients
- Medical records review
- Customer service
- Collecting debts
Four Steps to Compliance
Four Steps to Compliance

In order to comply with this Federal law, we take the following four steps:

(1) Identify the Red Flags for our business
(2) Set up procedures to detect Red Flags
(3) Respond to Red Flags to prevent theft or mitigate harm done
(4) Update our Identity Theft Detection and Prevention Program as needed to keep it current, and educate staff
Step One: Identify Red Flags
Step One: Identify Red Flags

Four Categories

University Specialty Clinics® has identified Red Flags that may be encountered in our day-to-day operations. Red Flags fall into four categories:

1. Presentation of suspicious documents
2. Presentation of suspicious personal identifying information
3. Suspicious account activity
4. Notice from other sources
Step One: Identify Red Flags

Category 1: Suspicious documents

- The person presenting the identification doesn’t look like the photograph or match the physical description.

- Documents provided for identification appear to have been altered or forged, or give the appearance of having been destroyed and reassembled.
Step One: Identify Red Flags

Category 1: Suspicious documents

Information on the identification differs from what the person presenting the information is telling you.

Information on the identification is not consistent with readily accessible information that is on file with University Specialty Clinics®, such as a registration signature.
Step One: Identify Red Flags

Category 2: Suspicious personal identifying information

個人識別情報が既知の詐欺活動と関連していることが示唆される、内部または第三者情報ソースを用いてUniversity Specialty Clinics®が指示した場合。例えば、システムに登録されている住所は、不正ドキュメントに記載されている住所と一致している例があります。
Step One: Identify Red Flags

Important Definition

“Identifying information” means “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any –

(1) Name, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
Step One: Identify Red Flags

Important Definition

(2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(3) Unique electronic identification number, address, or routing code; or

(4) Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e))."
Step One: Identify Red Flags

Category 2: Suspicious personal identifying information

個人識別情報が偽情報をがらの行為にしばしば関連されていることを示しています。たとえば、申請書の住所が偽である；または、電話番号が無効である、又は、ペイジーサービスまたはメッセージングサービスに関連しています。
Step One: Identify Red Flags

Category 2: Suspicious personal identifying information

The SSN provided is the same as that submitted by another patient, or the SSN is invalid:

- The first three digits are in the 800, 900, or 000 range, are in the 700 range above 772, or are 666;
- The fourth and fifth digits are 00; or
- The last four digits are 0000
Step One: Identify Red Flags

Category 2: Suspicious personal identifying information

⚠️ The person opening the covered account or the patient fails to provide all required personal identifying information on registration and doesn’t respond to notification that the registration is incomplete.

⚠️ Personal identifying information provided is not consistent with that which is on file with University Specialty Clinics®. For example, the signature does not match that which is on file.
Step One: Identify Red Flags

Category 2: Suspicious personal identifying information

The patient cannot provide authenticating information or the answer to challenge questions beyond that which generally would be available from a wallet or consumer report.
Step One: Identify Red Flags

**Category 3: Suspicious account activity**

- Mail sent to the patient is returned repeatedly as undeliverable, although transactions continue to be conducted in connection with the patient’s account.
- University Specialty Clinics® is notified that the patient is not receiving paper account statements in the mail.
Step One: Identify Red Flags

Category 3: Suspicious account activity

University Specialty Clinics® is notified of unauthorized transactions in connection with a patient’s account.

The account shows unusual activities (inconsistent with established patterns); e.g., non-payment when there is no history of late or missed payments.
Step One: Identify Red Flags

Category 3: Suspicious account activity

- The patient’s medical record shows medical treatment or health care services that are inconsistent with a physical examination or with a medical history as reported by the patient.
- The patient has an insurance number but never produces an insurance card or other insurance documentation verification.
Step One: Identify Red Flags

Category 4: Notice from other sources

University Specialty Clinics® may receive notice from patients, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft. For example:

The patient complains, after accessing a copy of their medical record, that the record contains documentation regarding a health care diagnosis or treatment that the patient denies ever having.
Step One: Identify Red Flags

Category 4: Notice from other sources

⚠️ The patient complains or has questions based on the patient’s receipt of:

* a bill for another individual;
* a bill for a product or service that the patient denies receiving;
* a bill from a health care provider that the patient never visited;
* an explanation of benefits (EOB) for health care services never received; or
* collection notices from a bill collector for services never received.
Step One: Identify Red Flags

Category 4: Notice from other sources

- The patient or patient’s insurance company reports
  - that coverage is denied because insurance benefits have been depleted or a lifetime cap has been reached, or
  - that coverage for certain health care services is denied due to a diagnosis or health care condition that the patient denies ever having.
Step One: Identify Red Flags

Category 4: Notice from other sources

University Specialty Clinics® receives complaints or questions concerning information added to a credit report by a health care provider or insurer.

The patient disputes a bill by claiming to be the victim of identity theft.
Step One: Identify Red Flags

Category 4: Notice from other sources

University Specialty Clinics® receives a notice of inquiry from an insurance fraud investigator for an insurance company or a law enforcement agency.

University Specialty Clinics® receives police reports or investigations regarding a patient’s identity theft case.
Step Two: Detect Red Flags
Step Two: Detect Red Flags

University Specialty Clinics® personnel should exercise due diligence in the detection of Red Flags by following their Department’s procedures for verification of identity and authority when processing a new patient registration and when verifying the identity of an existing patient; and by being alert for Red Flags in day-to-day operations.
Step Two: Detect Red Flags

If patients ask the reason for our identifying procedures, personnel should explain that the procedures are “for patient protection to help prevent identity theft.”
Step Three: Prevent and Mitigate Identity Theft
Step Three: Prevent and Mitigate Identity Theft

Notify your supervisor and/or the Department’s Administrative Director when you encounter

- suspicious documents,
- suspicious personal identifying info,
- suspicious account activity;

or receive

- notice of Red Flags or identity theft from other sources.
Step Three: Prevent and Mitigate Identity Theft

If you receive a discrepancy report from a patient, a victim of identity theft, a law enforcement official, or other individual that indicates a Red Flag or identity theft:

* Request they supply a written report to the Department.
* Retain copies of documentation included with the report.
* Note the discrepancy report in the patient’s medical record and billing record.
Step Three: Prevent and Mitigate Identity Theft

Depending on the perceived degree of risk, your Department’s, and/or University Specialty Clinics®, response to a detected Red Flag may include one or more of the following:

* Monitoring the patient’s account for evidence of identity theft
* Contacting the patient
Step Three: Prevent and Mitigate Identity Theft

Possible Responses (cont’d):
* Advising the patient to report the identity theft to the local police and provide a copy of the police report to University Specialty Clinics®
* Changing any passwords, security codes, or other security devices that permit access to a covered account
Step Three: Prevent and Mitigate Identity Theft

Possible Responses (cont’d):
* Re-opening a covered account with a new account number, declining to open a new account, or closing an existing account
* Not attempting to collect on a covered account or not selling a covered account to a debt collector
* Notifying law enforcement
Step Three: Prevent and Mitigate Identity Theft

Possible Responses (cont’d):

* Determining that no response is warranted under the particular circumstances (when University Specialty Clinics® determines that the Red Flag did not evidence a risk of identity theft)

* Placing the covered account “on hold” from any further access, use, or disclosure until the Red Flag event is fully investigated
Step Three: Prevent and Mitigate Identity Theft

Possible Responses (cont’d):
* Isolating and correcting inaccuracies in medical records resulting from identity theft
Step Three: Prevent and Mitigate Identity Theft

It’s anticipated that most investigation and resolution of detected Red Flags will remain at the Department level.

Where there is a strong indication of identity theft, the Administrative Director will fax a completed HIPAA Privacy/Security and Red Flags Incident Report form to the HIPAA Privacy Officer (fax 803-255-3439) or to the Office of Legal Affairs (fax 803-255-3435).
The University Specialty Clinics® HIPAA Privacy/Security and Red Flags Incident Report form is available on the University Specialty Clinics’® Web page.
Step Three: Prevent and Mitigate Identity Theft

If identity theft is alleged by the patient, request that the patient complete and return the FTC Identity Theft Affidavit, and advise the patient to report the identity theft incident to law enforcement.
Step Three: Prevent and Mitigate Identity Theft

The following link to the FTC Identity Theft Affidavit is available on the University Specialty Clinics’® Web site:

http://www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf

Please fax a copy of any FTC Affidavits that are received to the HIPAA Privacy Officer:
Fax (803) 255-3439
Step Four: Update the Program

The Office of Legal Affairs and the HIPAA Privacy Officer provide oversight for our Identity Theft Prevention and Detection Program.
Step Four: Update the Program

An annual report will be provided to the Privacy and Security Advisory Committee that addresses

* the effectiveness of our Program,
* monitoring of service provider arrangements,
* significant incident reports and our responses, and
* recommendations for Program changes.
University Specialty Clinics®

Identity Theft Prevention and Detection Program Resources
Identity Theft Prevention and Detection Program Resources

Each clinical department maintains at least one printed copy of:

- The University Specialty Clinics® Identity Theft Prevention and Detection Program, Policy and Procedures, effective 05/01/09
- The training PowerPoint and training attestation statement
- The FTC Identity Theft Affidavit form
- The HIPAA Privacy/Security and Red Flags Incident Report form
Identity Theft Prevention and Detection Program Resources

Materials related to our identity theft prevention and detection program are also maintained on the University Specialty Clinics’® Web site.

Questions about our Program should be relayed to the HIPAA Privacy Officer (255-3454), or to the Office of Legal Affairs (255-3432).
Service Providers
Service Providers

The Red Flags Rule requires creditors to “exercise appropriate and effective oversight of Service Provider arrangements.”
Service Providers

Important Definition

A “Service Provider” is an entity that provides a service directly to University Specialty Clinics® or one of its Departments and is in a position to identify and report a Red Flag to University Specialty Clinics® in the normal course of business.

The Office of Legal Affairs will oversee Service Provider arrangements to ensure that such arrangements comply with the Red Flags Rule.
Service Providers

Current Contracts

Initially, the Office of Legal Affairs will review all current University Specialty Clinics® agreements to identify contractors that meet the definition of “Service Provider.”

Each Service Provider contract will be amended to require that the Service Provider’s activities are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.
Service Providers

Future Contracts

Future Service Provider arrangements will include an updated Business Associate Agreement that includes language addressing the Red Flags Rule.

The Office of Legal Affairs will provide each Department with the updated Business Associate Agreement template.
Questions?

Please e-mail any questions you may have about information in this training PowerPoint to:

HIPAA Privacy Officer:
Susan.Hartnett@uscmed.sc.edu

Office of Legal Affairs:
Alicia.Schlachta@uscmed.sc.edu