UCLA Faculty Practice Group

"RED FLAGS RULE"

GENERAL INFORMATION

UCLA Faculty Practice Group

What Is The Purpose Of "Red Flags Rule"?

In November 2007, the Federal Trade Commission (FTC) issued regulations requiring that certain entities develop and implement identity theft prevention and detection programs to protect consumers from identity theft. The implementation deadline is June 01, 2010.

The program must include a mechanism for:

- Prevention
- Detection
- Response

UCLA Faculty Practice Group

What Is The Purpose Of "Red Flags Rule"?

Identity theft occurs when someone uses another's personal identifying information (e.g. name, SSN, credit card number, or insurance/coverage data) to commit fraud or other crimes.

Medical identity theft occurs when someone uses a person's name, insurance information, etc., without that person's knowledge to obtain or make false claims for medical services or goods.

Who Has To Comply With The "Red Flags Rule"?

The FTC takes the position that the physicians extend credit to patients by allowing deferred payments until the services are rendered and insurance is collected (or monthly payment plans are established with the patients).

Even though AMA does not agree with this position and actively lobbies against this rule, physicians are still required to comply by June 01, 2010 or face penalties of up to $2,500 per known violation.

How Does This Rule Defer From HIPAA Security And Privacy Rules?

HIPAA is intended to protect personal health information (PHI). Although, PHI is covered by the "Red Flags Rule", the latter extends to other sensitive information:

- Credit card information
- TIN, SSN, Employer ID, etc.
- Insurance claim information

UCLA Faculty Practice Group

What Is A "Red Flag"?

A Red Flag is a pattern, practice, or specific account activity that indicates the possibility of identity theft. The FTC identifies the following as red flags:

- Alerts, notifications or warnings from a consumer reporting agency
- Suspicious documents and/or personal identification information, such as an inconsistent address or non-existent SSN
- Unusual use of, or suspicious activity relating to a patient's account
- Notices of possible identity theft from the patients, victims of identity theft or law enforcement authorities

UCLA Faculty Practice Group

"RED FLAGS RULE"

What You Need To Know, and What You Need To Do?

UCLA Faculty Practice Group

What You Need To Know, and What You Need To Do?

PREVENTION

Contact Via Phone:

A. Request an account number and the name of the caller

- Sample script, "May I have your account number and name?"
- Obtain caller's full name so when you pull up the account number you can easily see if the caller is the patient.

B. Verify caller by requesting at least 2 identifiers

- Last four digits of SSN
- Date of Birth

What You Need To Know, and What You Need To Do?

PREVENTION

C. If the name of the caller and the account number are different, ask “What is your relationship to the patient?”

- If self (patient calling), request and verify the following (must answer 2 of the 3):
  - Current address and phone number
  - Maiden name and/or AKA (if available)
  - DOS

UCLA Faculty Practice Group

What You Need To Know, and What You Need To Do?

PREVENTION

- If it is not the patient calling, ask for the following: (must answer 2 of the 3):
  - Last 4 digits of the SSN of the patient
  - Patient's date of birth
  - Patient's address
- If the caller is unable to verify 2 of the 3 identifiers and there is concern of possible identity/medical identity theft, escalate to supervisor/manager

UCLA Faculty Practice Group

What You Need To Know, and What You Need To Do?

DETECTION

Same name or DOB, with different SSN

Different first name, with same last name or vice versa, but with the same SSN

Multiple hyphenated names and they are given in different orders, or the name is not consistent with prior visits

UCLA Faculty Practice Group

What You Need To Know, and What You Need To Do?

DETECTION

Patient admits to using another person's identity for services

Patient receives bills, EOBs or a collection notice for medical services that were not received

Patient notified of medical data breach

UCLA Faculty Practice Group

What You Need To Know, and What You Need To Do?

DETECTION

Complaint or question from a patient based on the patient's receipt of a bill for another individual

Complaint or question from a patient about information added to a credit report by a health care provider (unpaid bill)

Notices from consumers, law enforcement or others of unusual activity related to the accounts

UCLA Faculty Practice Group

What You Need To Know, and What You Need To Do?

RESPONSE

- Tell the patient/caller that you need to do further investigation of the account and he/she will receive a call back
- Notify the supervisor/manager immediately
- The supervisor/manager should attempt to resolve obvious registration issues (e.g., change of address, maiden name)
- The supervisor/manager will call the patient for verification of identification
- Review with the patient the importance of correct identification and patient safety

UCLA Faculty Practice Group

What You Need To Know, and What You Need To Do?

RESPONSE

- **Document any refusal to comply in SIGNATURE notes**
- **If after speaking with the patient, the patient presents different information, proceed to gather the new information and process verification as per usual protocol, documenting interventions**
- **If the situation requires further investigation the manager should notify the UCLA Medical Sciences Compliance Officer (310-794-0922)**

UCLA Faculty Practice Group

What You Need To Know?

RESPONSE

- **The UCLA Medical Sciences Compliance Officer will coordinate the investigation of potential identity theft incidents and will involve as necessary:**
  - **Risk Management**
  - **Legal Affairs**
  - **Privacy Officer**
  - **Patient Admissions and Registration-To apply any applicable alerts**
  - **Medical Records - Who after determination of identity theft will implement their departmental process for rectifying the Patient Record as appropriate**
  - **Information Security Officer**
  - **UCPD**

SCENARIOS

UCLA Faculty Practice Group

Scenarios

RED FLAG 	DETECTION	REQUIRED RESPONSE	RESOLUTION
Caller, self-identifying as patient, needing or wanting to discuss account but is unable to validate certain identifiers on the account.	Caller must be able to validate at least 2 identifiers, including patient account number, DOB, last 4 digits of SSN, current address, maiden name, etc.	No assistance without assured verification of identity.	A persistent request is referred to Supervisor/Manager. Patient will be contacted after review.

Scenarios

RED FLAG 	DETECTION	REQUIRED RESPONSE	RESOLUTION
Caller, self-identifying as family member/third party, needing or wanting to discuss the account, but is unable to validate certain identifiers on the account	Caller must be 1. able to validate at least 2 patient identifiers, including patient account number, DOB, last 4 digits of SSN, current address, maiden name, etc., or 2. have valid Release of Information documentation (HIPPA compliant) AND/OR is identified in systems as spouse, guardian, etc.	No assistance without assured verification of identity. * If the call is from insurance company/payor, caller must be able to identify claim details. Provide only financial information.	A persistent request is referred to Supervisor / Manager.

UCLA Faculty Practice Group

Scenarios

RED FLAG 	DETECTION	REQUIRED RESPONSE	RESOLUTION
Caller, self-identifying as patient, requesting information change but is unable to validate certain identifiers on the account	Caller must be able to validate at least 2 identifiers, including patient account number, DOB, last 4 digits of SSN, current address, maiden name, etc.	No assistance without assured verification of identity.	A persistent request is referred to Supervisor / Manager. Patient will be contacted after review.

Scenarios

RED FLAG 	DETECTION	REQUIRED RESPONSE	RESOLUTION
Caller, self-identifying as family member/third party, requesting information change but is unable to validate certain identifiers on the account	Caller must be 1. able to validate at least 2 patient identifiers, including patient account number, DOB, last 4 digits of SSN, current address, maiden name, etc. 2. have valid Release of Information documentation (HIPPA compliant) AND/OR is identified in systems as spouse, guardian, etc.	No assistance without assured verification of identity. * If call is from insurance company / payor, caller must be able to identify claim detail. Provide only financial information.	A persistent request is referred to Supervisor/Manager.

UCLA Faculty Practice Group

Scenarios

RED FLAG 	DETECTION	REQUIRED RESPONSE	RESOLUTION
Caller, self identifying as patient or victim of potential theft	Caller should be able to give general information in regards to account	No assistance Obtain detail information. Notify Supervisor/Manager	Investigate and resolve with Supervisor / Manager
Caller, self-identifying as patient, requesting statement but is unable to validate certain identifiers on the account	Caller must be able to validate at least 2 identifiers, including patient account number, DOB, last 4 digits of SSN, current address, maiden name, etc.	No assistance without assured verification of identity.	A persistent request is referred to Supervisor / Manager. Patient will be contacted after review.

This presentation and other helpful references on FPG PBO policies and procedures website at:

www.fpg.mednet.ucla.edu

Log on: pbopolicy

Password: pbopolicy

QUESTIONS ???