

“Red Flag Rules” – Identity Theft Prevention Program



Training for Providers and Staff in Healthcare

Presented by: Helen Hadley

President

VantagePoint HealthCare Advisors

History

- Identity Theft Regulations
- FACTA (Fair and Accurate Credit Transactions Act of 2003)
- Code of Federal Regulations
- Implementation Date: November 1, 2009
- Oversight by FTC (Federal Trade Commission)

Purpose of Red Flags Rule

- To make reasonable attempts to prevent and detect identity theft through a formal prevention program and to respond appropriately to mitigate the theft
- This is NOT HIPAA
- Medical practices should be diligent in preventing theft of “Personal Identifying Information”

Definitions: “Medical Identity Theft”

- Medical Identity Theft - occurs when someone uses a person’s name and sometimes other parts of their identity -- such as insurance information -- without the person’s knowledge or consent to obtain medical services or goods, or uses the person’s identity information to make false claims for medical services or goods. Medical identity theft frequently results in erroneous entries being put into existing medical records, and can involve the creation of fictitious medical records in the victim’s name. (World Privacy Forum)

Definitions - “Covered Account”

- Covered Account: Any account that...involves multiple payments or transactions including one or more deferred payments, and
 - Any other account for which there is a reasonably foreseeable risk from identity theft

Definitions: “Identity Theft”

- Identity Theft: fraud committed using the identifying information of another person



Definitions: “Creditor”

- Creditor: any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.
- Healthcare providers extend credit to patients and are therefore, considered “creditors”.

Definitions: Service Provider

- A *service provider* is a person or entity that provides a service directly to the financial institution or creditor
- A practice's service providers may include:
 - Billing companies
 - Consultants
 - Attorney
 - Accountant
 - Transcription Company
 - EMR Vendor
 - Collection Agency



Definitions: “Red Flag”

- Red Flag: a pattern, practice, or specific activity that indicates the possible existence of identity theft

Red Flags

- Identity Theft Prevention is known as the Red Flags Rule
- Intention is to provide consumers (our patients) with protection from identity theft

Red Flags Rules

- A set of rules centered on preventing and detecting identity theft

Requirements

- “Creditors” with “covered accounts” must develop a written identity theft prevention program
- In connection with the opening of a (new) covered account or any existing account, the program must include policies to:
 - Detect Identity Theft
 - Prevent Identity Theft
 - Mitigate Identity Theft

Application in Healthcare

- Under the rule, healthcare providers are considered “creditors”
- Under the rule, patient accounts are considered “covered accounts”
- Healthcare providers meet the definition because patients are allowed to defer payments (even when claims are submitted for payment to a third party such as an insurance company)

Application in Healthcare Entities

- Programs and policies can be flexible and tailored to the size and complexity of the organization

Requirements

- Federal Trade Commission (FTC) expects the healthcare entity to:
 - Conduct a risk assessment to determine the risks within the entity
 - Develop written policies regarding how the entity will identify and respond to suspicious practices that may lead to identity theft

Requirements

- Must obtain board approval of the (initial) written policy
- Must implement the policy within the organization
- Must periodically review, update and revise the policies

Program Elements

- The healthcare entity must establish policies and procedures to:
 - Identify relevant red flags and incorporate them into the program
 - Detect red flags that are part of the program
 - Respond appropriately to any red flags that are detected
 - Ensure the program is updated periodically to address changes

Oversight of the Program

- Initial approval from the board is required
- Someone should be identified to oversee the program
- Staff must be trained
- Service provider arrangements require oversight

Awareness of Red Flags

- Everyone in the healthcare organization must be aware of the “red flags” that point to possible identity theft

Awareness of Red Flags

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers
- Presentation of suspicious documents
- Presentation of suspicious personal identifying information (“PII”)
- Unusual use of, or other suspicious activity related to a covered account
- Notice from patients, victims of identity theft, or law enforcement authorities

Ways to Detect Red Flags

- Verify patient's identity at registration (ask for more than one form of ID)
- Authenticate patients
 - “What is your current address?”
 - “What is your date of birth?”
- Monitor transactions
 - Billing office staff should be diligent about who is asking what about the account
 - Billing office staff should watch names/address on checks to ensure they match with patient account
- Verify validity of patients address changes
 - Registration staff should be alert to suspicious patients

Registration

- A key opportunity to ensure that patient is appropriately identified
 - Do you already know the patient?
- Request & copy driver's license or other photo ID
 - If no photo ID, you may ask for utility bill or other correspondence showing current address
- Request & copy insurance ID card
- Update registration forms every six months

Watch for discrepancies

- Any information (license, photo ID, insurance card) appears altered
- Photo ID does not look like patient
- Match all information on check to the patient
- Look at phone numbers, also
- Inconsistent information when you compare documents
- Post office box is provided without street address
- Invalid phone numbers should be flagged in accounts
- Patient complaints/inquiries from patients
- Patient's signature does not match that on documents
- Report suspicions to management

The FTC's 26 Red Flags

1. A fraud alert included with a consumer report (probably not applicable to medical practices)
2. Notice of a credit freeze in response to a request for a consumer report (also probably not applicable in medical practices)
3. A consumer-reporting agency providing a notice of address discrepancy
4. Unusual credit activity, such as an increased number of accounts or inquiries
5. Documents provided for identification appearing altered or forged

FTC's 26 Red Flags con't

6. Photograph on ID inconsistent with appearance of customer (patient)
7. Information on ID inconsistent with information provided by person opening account
8. Information on ID, such as signature, inconsistent with information on file
9. Application appearing forged or altered or destroyed and reassembled (look closely at ID cards, SS cards, Insurance ID cards)
10. Information on ID not matching any address in the consumer report; SSN has not been issued or appears on SS Death Master file
11. Lack of correlation between SSN range and date of birth
12. Personal identifying information associated with known fraud activity

FTC's 26 Red Flags con't

13. Suspicious addresses supplied, such as mail drop or prison, or phone numbers associated with answering services or pagers
14. SSN provided matching that submitted by another person opening an account (if possible, do a SSN search when registering patients)
15. An address or phone number matching that supplied by a large number of applicants (if possible, so a phone number search when registering patients)
16. The person opening the account is unable to supply identifying information in response to notification that the application ("registration information") is incomplete
17. Personal information inconsistent with information already on file
18. Person opening account or customer unable to correctly answer challenge questions ("What is your date of birth? Current address? Phone number?")
19. Shortly after change of address, creditor receiving request for additional users of account

FTC's 26 Red Flags con't

20. NA

21. Drastic change in payment patterns

22. NA

23. Mail sent to patient repeatedly returned as undeliverable despite ongoing transactions on active account

24. Notification that customer is not receiving paper account statements

25. Notification (by patient) of unauthorized charges or transactions on account

26. Notification that a fraudulent account has been opened for a person engaged in identity theft

Methods for Responding

- Monitor patient accounts
- Contact patients
- Change passwords
- Close compromised account
- Reopen accounts (new number)
- Refuse to open account
- Stop collecting on questionable account
- Do not turn account over to debt collector
- Remove false information from records
- Notify law enforcement
- Do nothing (no response warranted)

Identity Thieves

- Can be internal
 - Employees who have access to patient medical records and patient accounts
 - Others who have access to medical records and patient accounts but are not employees
 - Your collection agency
 - Transcriptionist
 - Billing Company
 - Maintenance Crew
 - Etc, etc...

Identity Thieves

- Can be external
 - Someone posing as a friend or relative of the patient
 - In person
 - Via phone/email
 - Someone posing as the patient

Summary

- Abide by the regulations
- Policies & procedures must be in writing
- Be alert to patients during the registration process
- Be alert to activity surrounding patient accounts
- Keep medical records (paper and electronic) secure!
- Report suspicious activities to management

Wrap Up

- Q&A

Disclaimer

VantagePoint made very effort to ensure the accuracy of the materials presented. However, VantagePoint makes no guarantee, warranty or representation that the information contained herein is accurate, complete, or without errors. It is further understood that VantagePoint, its' employee and subcontractors, are not rendering any legal or other professional services or advice. VantagePoint, its' employees and subcontractors bear no liability for any results or consequences that may arise from the use and distribution of the information in this presentation.

VantagePoint

- Compliance Programs
- Operational Assessment
- Revenue Enhancement
- Accounts Receivable Management
 - Interim Practice Management
- Coding/Medical Record Audits
 - HIPAA Privacy/Security
 - Project Management
 - Strategic Planning
- EMR Selection/Implementation
- Red Flags Identity Theft Prevention Program



www.vantagepointconsult.com hhadley@vantagepointconsult.com

Hamden, Connecticut

Rochester, New York

203-288-6860