



The Red Flag Rules: Ready or Not – Here They Come!

A Presentation for Members by The Nebraska Medical Association

Jill Jensen, J.D.

Cline, Williams, Wright, Johnson & Oldfather, L.L.P.

March 31, 2009

Law Firm of

Cline, Williams, Wright, Johnson & Oldfather, L.L.P.

Quality Legal Representation since 1857

What are the “Red Flag Rules”?

- Require written identity theft prevention programs to
 - Identify,
 - Detect, and
 - Mitigate identity theft



What is a “Red Flag”?

- A pattern, practice, or activity that indicates the possible existence of identity theft



Who is Affected by the Red Flag Rules?

- Financial Institutions
- Creditors
- Users of Consumer Reports



Creditors with “Covered Accounts”

- Any person who regularly extends, renews, or continues credit;
- Who regularly arranges for the extension, renewal, or continuation of credit; or
- Any assignee of an original creditor

“Covered Accounts”

An account (a continuing relationship established by a person) that a creditor offers or maintains primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions,



What Must You Do?

- **Develop and implement a written program with policies and procedures to “detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.”**

What is “Identity Theft”?

- **Fraud** committed or attempted
- Through the use of **identifying information**
- Of **another person** (individual or entity)
- **Without permission**





Oh, no!

Not HIPAA again!



First

- **Develop and implement a written program with policies and procedures to “detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.”**

Include in Your Program:

- **Reasonable policies and procedures** to help you
 - **Identify** relevant Red Flags for your covered accounts
 - **Detect** the Red Flags you identify
 - **Respond** appropriately to prevent and mitigate identity theft
- **Update** your program's policies and procedures periodically
- Provide **periodic (at least yearly) reports** to management

Identifying Red Flags

- From incidents of identity theft at your clinic or anecdotal
- Identity theft risks
- From governmental guidance



Key Point

- Consider which Red Flags are likely to affect your covered accounts
- Incorporate into your security practices/procedures



What Else is Required?

- Get your program approved by your “Board of Directors”
- Assign a Board member or someone in senior management to oversee, implement, and administer the program



What Else?

- Train Staff
- Work with service providers
 - Exercise oversight of arrangements with them
- Review current business associate arrangements

What Must You Do?

- Develop and implement a written program with policies and procedures to “**detect, prevent, and mitigate identity theft** in connection with the opening of a covered account or any existing covered account.”

Once Your Program is in Place,

- **Monitor** covered accounts for identity theft (prevent/detect)
- **Notify** patients if needed (mitigate)
- **Act:** Change passwords, security codes, or take other security precautions



“Red Flags”

- **Suspicious documents:**
 - Insurance card that appears to be altered or forged
 - “Recycled” or shared insurance cards



“Red Flags”

- **Driver’s License Red Flags**
 - No match photo -- does not look like the patient
 - Physical description does not match the patient
 - Data discrepancies between your records and driver’s license
 - No match signature



More “Red Flags”

- **Information discrepancies:**
 - No match address, phone
 - Non-existent addresses or PO Box
 - Invalid Social Security Number
 - Patient refuses to provide personal identifying information or documents



Mitigation

- Reopening account with a new number
- Not opening a new account
- Close an existing account
- Not attempting to collect an account



Mitigation

- Not send an account to collections
- Notify law enforcement
- Determine that no response needed



What To Do if a Patient Claims Identity Theft?

- Patient receives an EOB and notices charges for services they never received
- Patient does not receive EOB, but calls you when the account is sent to collections



Ask Patient for

- Police report
- A copy of their Federal Trade Commission ID Theft Affidavit
- Copies of patient's driver's license or other photo ID
- Documentation of address
- Any facts known about the identity theft
- Other related information

How Will Your Office Respond to Identity Theft?

- ✓ Remove related charges from account
- ✓ Correct adverse credit report if by notifying consumer reporting agencies
- ✓ Segregate medical record information from the identity theft into a Jane/John Doe record



Compliance Keys

- Compliance required by May 1, 2009
- Review your current policies and procedures and make appropriate changes
- Get help from your practice's attorney



Compliance Keys

- Written program
 - Identify
 - Detect
 - Respond
- Approved by Board
- Administered by senior management
- Train staff
- Update as needed



Why Bother?

- Civil money penalties – each violation
- Negative publicity
- Potential civil liability



Resources

- www.ftc.gov
- See “Quick Finder” box on home page
- Click on “Identity Theft” tab
- See links on right side of page for resources
- See drop-down menu under “Businesses”



