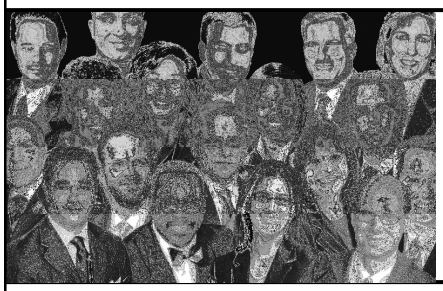

Pepper Hamilton LLP
Attorneys at Law

Identity Theft Prevention: The FTC's Red Flags Rules and Health Care Providers

HCCA Physician Practice Compliance Conference
October 13, 2009

Rebekah A. Z. Monson
Pepper Hamilton LLP
215.981.4031
monsonr@pepperlaw.com

Today's Discussion

- What is medical identity theft?
- What are the Red Flags Rules?
- Who do the Red Flags Rules apply to?
- What goes into an Identity Theft Prevention Program?
- Where do the Red Flags Rules fit?

2

Identity Theft

- Identity theft = “a fraud committed or attempted using the identifying information of another person without authority” (16 C.F.R. §603.2(a))
- “Identifying Information”
  - Name, SSN, DOB, driver’s license number, passport number, employer or taxpayer identification number
  - Unique biometric data
  - Unique electronic identification number, address or routing code

3

Identity Theft

- Financial identity theft
  - Impact on victims
  - Impact on providers
- Medical identity theft = use of a person’s information without knowledge or consent to obtain health care services, items or reimbursement
  - Financial impact
  - Impact on medical identity

4

Medical Identity Theft

- Uncertain statistics
- February 2008 FTC Report
  - Over 800,000 complaints
  - 32% categorized as identity theft
  - Approximately 2% attributed to medical
- Identity Theft Resource Center
  - 2008 reported data breaches increased 47% over 2007
  - 14.8% of reported breaches in health/medical

5

Red Flags Rules

- Fair and Accurate Credit Transactions Act of 2003 (FACT Act), which amended the Fair Credit Reporting Act (FCRA)
- Jointly issued regulations
- Issued on November 9, 2007 (72 Federal Register 63718)
- Mandatory compliance date of November 1, 2008 (delayed until November 1, 2009)

6

Red Flags Rules

- Applies to “financial institutions” and “creditors” with “covered accounts”
- Required to develop and implement a written Identity Theft Prevention Program
- “Red Flag” = pattern, practice, or specific activity that indicates the possible existence of identity theft
- 16 C.F.R. §681.2 and Appendix A to Part 681

7

Other Regulations

- Duties of credit and debit card issuers regarding changes of address (16 C.F.R. §681.3)
- Duties of users of consumer reports regarding address discrepancies (16 C.F.R. §681.1)

8

Notices of Address Discrepancy

- Applies to: “users” of “consumer reports” that receive a “notice of address discrepancy” from a “nationwide consumer reporting agency”
- “Notice of address discrepancy”
- Policies and procedures
  - “Reasonable belief” that same consumer
  - Furnishing consumer address to the NCRA

9

Identity Theft Prevention Program

- Who must implement a Program?
  - “financial institutions” and “creditors” that offer or maintain “covered accounts”
- Two step analysis:
  - (1) financial institution or a creditor?
  - (2) offer or maintain covered accounts?
- Do (and how) the Red Flags Rules apply to health care providers?
  - Application of FCRA

10

Step One: "Financial Institution"

- "Financial Institution" – defined to include:
  - banks
  - savings and loan associations
  - mutual savings banks
  - credit unions
  - certain other lenders
- Few health care providers and institutions fit into this category

11

Step One: "Creditor"

"Creditor" is defined to include:

- 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.

12

Step One: "Creditor"

- "Credit" - the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment
- Creditors include:
  - banks
  - savings and loan associations
  - mutual savings banks
  - credit unions
  - auto dealers
  - mortgage brokers
  - utility companies
  - other lenders

13

Step One: "Creditor"

- Broad definition
- Red Flags Rules and medical identity theft
- Key: providing services or products not paid for in-full at the time the product is provided or the service is performed
- Health care billing practices

14

Step Two: "Covered Accounts"

- "Account" is a continuing relationship between a financial institution or creditor and a person to obtain a product or service for personal, family, household or business purposes.
  - extensions of credit (ex: purchasing property or services using a deferred payment)
  - deposit accounts

15

Step Two: "Covered Accounts"

- A "covered account" is either:
  - (i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account;

16

Step Two: “Covered Accounts”

- Or, a “covered account” is:
  - (ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

17

Step Two Revisited

- Periodic determination of whether a creditor offers or maintains covered accounts
- Risk assessment:
  - methods the creditor provides to open accounts
  - methods it provides to access accounts
  - previous experience with identity theft

18

Establishing a Program

- Flexible
- Scalable
- FTC Guidelines (Appendix A)
  - Must "consider" the Guidelines
  - Include in the Program those Guidelines which are appropriate
- Other applicable laws and regulations

19

Identity Theft Prevention Program

- "designed to detect, prevent and mitigate identity theft in connection with
  - opening a covered account or
  - any existing covered account"
- Include reasonable policies and procedures
- Need (should) not be stand-alone program

20

Identity Theft Prevention Program

- Four core elements to a Program
  - Identify
  - Detect
  - Respond
  - Update
- Program Administration
  - Program Approval
  - Program Oversight
  - Training
  - Oversight of Service Providers

21

Identify Red Flags

- Identify Red Flags
- Incorporate Red Flags into Program
- FTC Guidelines risk factors:
  - types of covered accounts
  - methods to open covered accounts
  - methods to access covered accounts
  - previous experience with identity theft
- Sources of Red Flags
  - incidents of identity theft, methods of identity theft reflecting change in risks, and supervisory guidance

22

Identify Red Flags

- Guidelines: Program "should" include relevant Red Flags from each of five categories
  - Alerts, notifications or warnings from a consumer reporting agency
  - Presentation of suspicious documents
  - Presentation of suspicious personal identifying information
  - Suspicious activity on an account
  - Notice from the patient, law enforcement or others on possible identity theft.
- Supplement A – 26 examples of Red Flags

23

Detect Red Flags

- Policies and procedures
- Opening new covered accounts
  - Identifying and verifying identity of person
- Maintaining existing covered accounts
  - Authenticating patients
  - Verifying change of address requests
  - Monitoring transactions

24

Respond to Red Flags

- Policies and procedures
- “Appropriate” response
- Aggravating factors
- Guidelines

25

Periodic Updating

- Policies and procedures
- Reflect changes in risks of identity theft to
  - patients, or
  - safety & soundness of the creditor
- Factors
  - types of accounts and business arrangements
  - Red Flags determined to be relevant
  - methods of identity theft
  - methods to detect, prevent and mitigate identity theft

26

Program Approval & Oversight

- Initial approval by either Board of Directors or an appropriate committee of the BOD
- Program oversight by Board, an appropriate committee or a designated member of senior management
- Oversight activities:
  - assign responsibility for Program implementation
  - review staff reports regarding compliance
  - approve material changes to the Program

27

Program Oversight

- Staff report on compliance “at least annually”
- Contents of Report
- “Periodic” determination of whether a creditor offers or maintains covered accounts

28

Training

- Train employees and staff
- Policies and procedures
- Detecting and responding to Red Flags
- Employees and staff instrumental in detecting and responding Red Flags
- Education – staff and community

29

Oversight of Service Providers

- Exercise “appropriate and effective oversight” of service providers
- Ensure service providers act in accordance with reasonable policies & procedures
  - Require compliance with their Program
  - In some cases service providers may comply with own Program

30

Enforcement Delay(s)

- Red Flags Rule effective on January 1, 2008
- Mandatory compliance by November 1, 2008
- October 2008 - FTC suspended enforcement until May 1, 2009
- April 30, 2009 – FTC extends enforcement delay until August 1, 2009
- July 29, 2009 – FTC again extends enforcement delay until November 1, 2009

31

Enforcement Delay(s)

- Only affects FTC's enforcement activities
- Liability exposure for non-compliance
- AMA/Specialty Boards – FTC correspondence
- U.S. House of Representatives Bill 2345
- FTC Guidance
- FTC Do-It-Yourself Program for Businesses at Low Risk For Identity Theft

32

Where Do the Red Flags Rules Fit?

- HIPAA Privacy & Security Requirements
- ARRA HITECH Act
  - Privacy & Security changes
  - Security breach notification
- State Breach Notification Laws
- Other privacy & security laws
- Program should not be developed in isolation

33

Steps to Take

1. Determine if organization covered by Red Flags Rules
2. Learn about Red Flags Rules
3. Establish team/committee
4. Obtain Board approval and designee for Program oversight
5. Create a Program and adopt Policies and Procedures

34

Steps to Take

6. Review and update other policies and procedures
7. Develop processes to investigate red flags
8. Train, train, train
9. Educate your community
10. Update HIPAA Business Associate Agreements and other service agreements
11. ”Periodically” update Program & policies

35

Resources

- http://www2.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml
- http://www2.ftc.gov/bcp/edu/microsites/redflagsrule/get-started.shtm
- http://www2.ftc.gov/opa/2009/06/redflags.shtm
- http://www2.ftc.gov/opa/2009/04/redflagsrule.shtm
- http://www2.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf
- http://www2.ftc.gov/bcp/edu/pubs/articles/art11.shtm
- http://www2.ftc.gov/opa/2008/10/redflags.shtm
- http://www2.ftc.gov/opa/2008/07/redflagsfyi.shtm
- http://www2.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm
- Sample policies prepared by trade associations - American Medical Association, American Hospital Association
- www.worldprivacyforum.org

36

Questions?

Rebekah A. Z. Monson
Pepper Hamilton LLP
215.981.4031
monsonr@pepperlaw.com

37