THE FTC “RED FLAGS” RULE

Combating Medical Identity Theft: Compliance for Healthcare Providers

Wallis S. Stromberg
Davis Graham & Stubbs LLP

Heather L. Kenney
Davis Graham & Stubbs LLP

May 20, 2009
GOAL: Reduce identity theft through early fraud detection.

December, 2003—Fair Accurate Credit Transactions Act (FACTA) was enacted to provide consumers increased protection against identity theft.

Regulations were published on November 9, 2007, became effective January 1, 2008, with a mandatory compliance date of November 1, 2008.

FTC regulations apply to many healthcare providers. [Found at: 16 C.F.R. Part 681.]
RED FLAGS RULE

BACKGROUND

- Have been effective since November 1, 2008, for financial institutions and creditors that are regulated by authorities other than the FTC.

- AMA questioned applicability to healthcare providers in Fall, 2008, prompting the FTC to delay the Rule’s effective date.

- Effective August 1, 2009, for healthcare providers.

- FTC’s goal: (1) Prevention and (2) Mitigation of Damage
MEDICAL IDENTITY THEFT

World Privacy Forum’s definition of 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 a victim’s name. ¹

WHO MUST COMPLY?

CREDITORS

- Any financial institution or *creditor* that holds a *covered account*.

- A *creditor* includes any entity that regularly defers payments for goods or services or arranges for the extension of credit.

- **Examples of Creditors under the Rule:**
  1. Provider regularly bills patients for medical services after they have been rendered.
  2. Provider regularly allows patients to set up payment plans after the completion of medical services.
WHO MUST COMPLY?
COVERED ACCOUNTS

A *covered account* is:

a. used primarily for personal, family, or household purposes (consumer account); *and*

b. involves multiple payments or transactions; *or*

c. any other account with a reasonably foreseeable risk of identity theft.
FTC STRATEGY

- Expansive Coverage

BUT

- Tailored Requirements
  - Risk-Based Rule
Covered entities must develop written policies and procedures to prevent, detect, and mitigate identity theft.

Should address (1) misappropriation of personally identifying information from the provider’s own records; (2) the use by an identity thief of information procured from the outside in order to fraudulently obtain medical services from the provider.

Program should be uniquely tailored to the size, complexity, nature of operations, and actual experience of each entity.

Guidelines are available at Appendix A to 16 C.F.R. Part 681.
POLICIES & PROCEDURES—
FOUR REQUIRED ELEMENTS

1. Identify patterns, practices, and specific activities that signal possible identity theft ("Red Flags").

   Examples:
   - Alerts, notifications or warnings from a consumer reporting agency
   - Suspicious documents and/or personal identifying information, such as an inconsistent address or nonexistent Social Security number
   - Unusual use of, or suspicious activity relating to, a patient account
   - Notices of possible identity theft from patients, victims of identity theft or law enforcement authorities
Policies & Procedures—Four Required Elements

2. *Detect* red flags

- Develop policies and procedures to detect red flags, e.g.:
  - Verify new patient information with proper identification.
  - Authenticate patients when they arrive for services.
  - Verify insurance information.
POLICIES & PROCEDURES—FOUR REQUIRED ELEMENTS

3. **Respond** accordingly to red flags
   - Provide for appropriate response to detected red flags.
   - Response should be proportionate with the degree of risk.
   - If necessary, ensure that patient’s medical record is corrected.

4. **Periodically** update the Program
   - Record how the program will be kept current.
   - Program should reflect changes in risks to patients from new methods of identity theft or from incidents of identity theft actually experienced.
ADMINISTERING THE PROGRAM—FOUR STEPS

1. Obtain approval from either the healthcare organization’s board of directors, an appropriate board committee, or if the organization doesn’t have a board, a senior employee.

2. Involve either the board, committee or senior management employee in implementing, administering and program oversight.
ADMINISTERING THE PROGRAM—FOUR STEPS

3. Train staff to properly execute the program’s requirements.

4. Oversee any service provider arrangements in order to ensure that the provider acts in a manner that is consistent with the organization’s identity theft prevention program.
FTC’S VIEW OF RULE’S IMPACT ON HEALTHCARE PROVIDERS

“Given the risk-based nature of the Rule’s requirements...we do not believe the Rule would impose significant burdens for most providers...” In many cases that risk may be minimal or non-existent, such that a simple and streamlined program would be adequate. For example, for most physicians in a low risk environment, an appropriate program might consist of checking a photo identification at the time services are sought and having appropriate procedures in place in the event the office is notified...that the consumer’s identity has been misused. Such procedures might include not trying to collect the debt from the true consumer or not reporting it on the consumer’s credit report, as well as ensuring that any medical information about the identity thief is maintained separately from information about the consumer.”
HIPAA AND THE RED FLAGS RULE

- Red Flags Rule intersects with HIPAA’s privacy and security requirements.

- HIPAA focuses on maintaining privacy and confidentiality and on securing protected health information—internal to provider. **Aimed at preventing the compromise of patient information.**

- Red Flags Rule focuses on recognizing evidence that at a third party is involved in medical identity theft or that the internal system has been breached. **Its aim is to prevent or mitigate the misuse of compromised information.**

- Implementing the Red Flags Rule involves securing a patient’s information from unauthorized access, part of which can be accomplished by following a provider’s HIPAA policies.

- Providers should review their current HIPAA policies and integrate the appropriate policies into their Red Flags program as appropriate.
PENALTIES FOR NONCOMPLIANCE

- FTC can seek up to $3,500 in civil monetary penalties per violation. (For repeated violations after an order to comply, the FTC could file a suit seeking several times that for each violation.)

- States are authorized to bring an action on behalf of their citizens and can recover up to $1,000 per violation, as well as attorneys’ fees.

- Affected patients can bring civil suit, seeking actual damages and attorneys’ fees for negligent violations.

- For willful noncompliance, patients can seek actual damages, plus punitive damages and attorneys’ fees.
Additional Resources


- FTC fill-in-the-blank form for entities at a low risk of identity theft. Can fill out online and print.

- Both are available at [http://ftc.gov/redflagsrule](http://ftc.gov/redflagsrule).
QUESTIONS?