Red Flag Alert: Identity Theft

SEVEN STEPS TO START PLANNING (IF YOU HAVEN'T ALREADY)

By James P. Trotter, III, CHBME

Billing companies have been required to comply with a multitude of regulations during the past decade and phrases such as "protected health information," "accounting of disclosures," and "requests for authorization" have become old, familiar melodies. The risks of noncompliance, however, have increased from simple audits and the occasional refund request to exclusion from government programs, loss of licensure, and criminal and civil litigation. And no rest for the weary!

Federal Trade Commission's Implementation of the Fair and Accurate Credit Transactions ("FACT") Act of 2003

"Identity theft" has become a significant concern that has been exacerbated by the explosive growth in Internet-based activity. The FTC first addressed identity theft in 2003 as a part of the FACT Act. Known as the "Red Flag Rules," expected implementation was November 1, 2008. At the time of this publication, it is likely that medical providers will be defined as "creditors" under the Rules and will thus be required to comply. That said, many medical organizations, including the HBMA, have submitted comments to the FTC contesting the application of the Red Flag Rules to medical providers, which resulted in a six-month delay in implementation to May 1, 2009. The Federal Trade Commission has announced a further delay until August 1, 2009.

The FTC defines a creditor as "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" (http://ftc.gov/os/fedreg/2007/november/071109redflags.pdf). Presuming medical providers will be required to comply with the Red Flag Rules, billing companies are advised to gear up for implementation.

At the core of the rules is the establishment of a program to detect, prevent, and mitigate identify theft. A "reasonable" standard for implementation applies to the Red Flag Rules, meaning an entity has discretion in developing policies and procedures it deems are reasonable based on the environment in which it works.

The goals of any Red Flag program should include:

a) identification of indicators of possible identity theft risk, i.e., the "red flags"

b) detection of red flags

c) process to mitigate identity theft

d) ongoing updates of the identity theft program

Presuming medical providers will be required to comply with the Red Flag Rules, billing companies are advised to gear up for implementation.

"Red flags" indicative of identity theft that a billing company might encounter include a patient's presentation of identification documents that appear to have been altered, photo identification that is inconsistent with a patient's appearance, and other inconsistent identifying information.

Identity Theft Prevention

Steps a billing company may consider taking in establishing an identity theft prevention program include:

1. Identify "Covered Accounts"

A "Covered Account" is any account

(continued on page 25)

Red Flag Alert: Identity Theft *(continued from page 24)*

offered or maintained by a provider to cover multiple transactions or payments where there is a foreseeable risk to consumers of "identity theft, including financial, operational, compliance, reputation, or litigation risks."

2. ***Perform a Risk Assessment and Document the Results***
   Billing companies should perform a risk assessment on behalf of their clients that includes a review of patient identity verification to open an account (detail the process at the doctor's office or at the hospital), a description of the information that is gathered, how that information is stored, and potential steps that could be taken to detect and prevent identity theft in connection with existing accounts.

   Of particular importance is credit card safety and billing companies need to consider how information is handled, whether over the phone, via the web or through the mail.

3. ***Develop Policies and Procedures***
   Once the risk assessment is complete, a billing company should review any relevant Red Flags that have been identified and the potential risk level for identity theft. The next step is to determine the appropriate responses which may vary and should be appropriate to both the risk level and the detected Red Flag.

4. ***Train Staff***
   All staff that access Covered Accounts must be trained regarding the policies and procedures applicable to their job functions. This includes training for newly hired employees, refresher training, and training on any new policies or procedures or when existing policies are updated.

5. ***Amend Service Provider Arrangements***
   Billing service contracts may need to be amended to demonstrate compliance with the Red Flag Rules.

6. ***Obtain Board Approval for Program Implementation***
   Ideally, the Board of Directors or other governing body should be involved with the development, implementation, and oversight of the program. At a minimum, Board review and approval is required.

7. ***Report Annually to the Board on the Program***
   Staff with the designated responsibility of program administration must report to the Board at least annually. The annual report should address:
   - Program policies and procedures
   - Service provider arrangements
   - Significant incidents of identity theft, if any
   - Responses taken to any detected incidents, as well as recommendations for any material changes to the program

Though an identity theft program may sound ambitious, billing companies will find that many program elements are likely already in place through compliance with the HIPAA Privacy and Security regulations.

Though an identity theft program may sound ambitious, billing companies will find that many program elements are likely already in place through compliance with the HIPAA Privacy and Security regulations. Many of the Red Flag policies and procedures will be duplicative of HIPAA policies, which should allow HBMA members to meet the extended deadline of compliance by August 1, 2009. ▲

James P. Trotter, III, CHBME, is chief operations officer for Management Services Network, LLC ("MSN") with headquarters in Columbus, Georgia. He can be reached at jtrotter@msnllc.com