

Real World Advice for the Healthcare Community on the Red Flag Rule

Many companies affected may be unaware of their obligations to comply with the Federal Trade Commission's (FTC) Red Flag Rules focusing on identity theft. Although this legislation was enacted last year and enforcement was scheduled to begin November 1, 2008, the FTC recently moved the enforcement date to May 1, 2009. The new enforcement date doesn't change the obligation to be compliant, only the FTC's ability to enforce the legislation.

This regulation may affect anyone providing services where the consumer is invoiced monthly or provides the consumer with a payment plan. The American Health Care Association and American Medical Association have confirmed that healthcare providers may have to comply. They say "may" because this regulation does not apply if you collect the entire fee before services are rendered. Many physicians collect a fee that represents the amount not covered by insurance (the deductible) and bill the insurance company for the remainder. If the insurance does not reimburse the entire amount and the provider invoices the patient, the provider then must comply with the Red Flag Rule.

The regulation was a joint rule from the Federal Trade Commission (FTC) & Federal Financial Institutions Examination Council (FFIEC). To read the full text of the regulation visit: <http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf>.

The purpose of the rule is to detect and stop identity thieves from using someone else's identifying information at your institution to commit fraud. A typical example might be a falsified insurance card to receive fraudulent benefits. This is distinct from data security regulations (like HIPAA or GLBA).

The regulation indicates that in order to comply you must

- Implement a written Identity Theft Prevention Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account (typically accepting a new patient) or any activity on the covered account.
- Identity Theft Prevention Program must be appropriate to the size and complexity of the financial institution or creditor, and the nature and scope of activities must include reasonable 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 changing risks.

A red flag is a pattern, practice, or specific activity that could indicate identity theft.

The policies that you should consider writing and implementing include:

- Overview Identity Theft Policy
- Registration (new client or patient acceptance)
- Red Flag Review
- Investigation of Suspected Identity Theft
- Disposition of Erroneous Records

The FFIEC has identified 26 financial red flags along with implementation guidelines. There are an additional 18 Red Flags if you translate the Financial Red Flags to Medical Red Flags. All 26 financial red flags do not necessarily need to be considered by the medical community, as there are about 10 financial red flags that deal with consumer reports and use of credit cards. There are five categories 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,
- Unusual use of, or other suspicious activity related to, a covered account, or
- Notice from customers, victims of identity theft, or law enforcement authorities.

The FFIEC estimated that it would take a financial institution approximately 41 hours of effort to comply. Experience has shown that in some cases the estimate was fairly close, however, for a larger organization with multiple locations, the estimate was represented only a fraction of the real effort. To comply, the FTC and FFIEC recommended the following activities (for more detail on these activities visit the full text of the ruling noted above):

- I. Incorporate existing policies and procedures
- II. Identify relevant red flags
- III. Procedures to detect red flags
- IV. Appropriate responses to red flags
- V. Periodic updating of the Program
- VI. Administering the Program
- VII. Other legal requirements

There are solutions available, including generic policy templates available for purchase on the internet, but they will require customization to your operation. For example, policies for a three person dental office will be less complex than a medical practice with multiple locations. The policies for a retirement home are different than those for a surgical hospital. So even if you purchase generic templates, plan additional effort to customize these templates. Also, make sure that training material is supplied if you go this route.

You can also contract with a consultant to perform a risk assessment at your location and they will customize the templates for your operation. This approach increases the probability of complying and decreases the amount of effort required by your staff.

Everyone usually wants to do the minimum there is to comply, however, one has to be prudent in selecting a cost effective approach while still complying with this or any regulation. While a simple approach to guard against Identify Theft may simply be to require a government issued identification, the regulation requires that the program is thought out, have the involvement of the highest levels in the organization and that the staff is trained appropriately.

Although it is true that the enforcement date has been moved to May 1, 2009, the effective date remained at January 1, 2008. The FTC penalties won't begin until May 1, 2009 and are currently set at \$2500/infracton and enforced by the state attorney general. Although we are not real sure how compliance will be monitored, the prudent approach is to comply with the regulation and combat Identity Theft and the corresponding negative publicity it could bring to your organization.

About Visage Solutions

Visage Solutions is a consulting company operating in the areas of regulatory compliance, risk assessment, information security and business continuity processes. For more information about Visage's Red Flag Solution, click <http://www.visagesolutions.com/RedFlagRule.htm>.