



RNews

Your Source for the Latest Industry News

FTC EXTENDS
ENFORCEMENT
DEADLINE FOR
IDENTITY THEFT
RED FLAGS
RULES

At the request of Members of Congress, the Federal Trade Commission (FTC) has announced that it is delaying enforcement of the "Red Flags" Rule until June 1, 2010. RSource is committed to providing updates on news that is vital to the hospital environment. The original news blast from RSource was sent prior to the earlier deadline of November 1, 2009, and it is included below for reference. The FTC extension of the enforcement date to June 1, 2010 was then announced, and RSource wants to ensure you're in the loop.

Hospitals are a part of the group of businesses and organizations required to comply with new Federal Trade Commission (FTC) rules for responding to signs of

possible identity theft. These rules were set to go into effect November 1, 2009.

The Identity Theft Red Flags Rule is an implementation of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act). The Red Flags Rule requires businesses and organizations to define procedures for detecting, preventing, and mitigating identity theft by identifying "Red Flags" that signal possible identity theft and then initiating appropriate actions. Hospitals are affected in several ways: as users of credit reports, as grantors of credit, and in response to potential identity theft. The Red Flags detect identity thieves presenting and using personal information at your institution. The purpose of the Red Flags is distinct from data security which is covered by HIPAA.

Hospitals are now required to have a program in place that:

- Identifies the types of red flags that are relevant
- Explains the process for detecting them
- Describes how the hospital will

**"Compliance with the Red
Flags Rule assures your
patients that you are
doing your part to fight
identity theft."**

respond to red flags to prevent **and** mitigate identity theft

- Details the steps that will be taken to keep the program current

What red flags signal identity theft? There is no standard checklist, but Supplement A to the Red Flags Rule, which is available at

<http://www.ftc.gov/redflagsrule>, sets out some examples. Here are a few warning signs that may be relevant to health care providers:

- Alerts, notifications, or warnings from a consumer reporting agency
- Suspicious documents
- Suspicious personally identifying information
- Suspicious activity relating to a covered account
- Notices from customers, victims of identity theft, law enforcement authorities, or other entities about possible identity theft in connection with covered accounts

Once your entity has identified its red flags that are relevant to its practice, the program should include the procedures put in place by the hospital to detect them in your day-to-day operations. Your program should also outline the steps the hospital has put in place to prevent and mitigate identity theft.

Regardless of how good your program looks on paper, the true test is how it works. According to the Red Flags Rule, your hospital program must be approved by the hospital board of directors. Or if your organization does not have a board of directors, the review and approval is completed by a senior employee. The Board or senior employee may also oversee the

administration of the program, including approving any important changes, or a senior employee may take on these duties. The program should outline how the staff will initially be trained, and then outline how it will ensure the program is updated periodically to address changing risks. Additionally, a hospital program should detail how your entity will monitor the work of your service providers and partners – for example, vendors that manage your patient billing or debt collection operations. Vendors are likely to have a Red Flags Rule program as well, so the hospital should consider confirming a program is in place and assessing how the program elements compare to your hospital program. The program is risk-based and flexible, and the key is to familiarize all members of your staff and appropriate affiliates with the rule and the new compliance procedures.

There are no criminal penalties in place for failing to comply with the rule; however, violators are subject to financial penalties. More importantly, compliance with the Red Flags Rule assures your patients that you are doing your part to fight identity theft.

If you're looking for more info about the Red Flags Rule, the FTC's Red Flag website, <http://www.ftc.gov/redflagsrule>, offers resources to help entities determine if they are covered and how to comply. The Commission has also posted FAQs that address how they intend to enforce the rule at <http://www.ftc.gov/bcp/edu/microsites/redflagsrule/faqs.shtm>.

RNews

