Health Information Compliance Alert

IDENTITY THEFT: Prepare for Red Flags Rule: Squelch Opportunities for Identity Theft

Implementation deadline is right around the corner. Does it apply to you -- and are you ready?

On May 1, the Federal Trade Commission will begin enforcing its "Red Flags Rule" for ensuring that businesses crack down on identity theft. Although many medical practices didn't feel that these rules applied to them, the government may feel otherwise. But we've got the tools that will help you prepare.

What is it? Under the Red Flags Rule, "certain businesses and organizations - including many doctor's offices, hospitals, and other health care providers - are required to spot and heed the red flags that often can be the telltale signs of identity theft," according to an article on the Federal Trade Commission's Web site. "To comply with the new Red Flags Rule ... you may need to develop a written 'red flags program' to prevent, detect, and minimize the damage from identity theft."

Who is affected? According to the FTC, the rule applies to businesses that qualify as "creditors" or "financial institutions." But don't take a sigh of relief just yet - the rule probably does apply to you.

"Health care providers are creditors if they bill consumers after their services are completed," the FTC Web site says. "Health care providers that accept insurance are considered creditors if the consumer ultimately is responsible for the medical fees. However, simply accepting credit cards as a form of payment does not make you a creditor under the rule."

How can you prepare? You should institute a red flag program in your practice, which you'll need to revisit at least annually and more often as needed, advises **Rebecca L.Williams, RN, JD,** with Davis Wright Tremaine in Seattle.

The rule requires you to develop a report that you'll submit to the board of directors (or to senior management),Williams says. "This report should include addressing the effectiveness of the program as well as significant incidents and responses of the organization."

Bottom line: You should identify which areas fall within the identity theft prevention programs, meaning all departments, multiple sites, etc.,and ensure that when you're developing your program, that it is designed to detect, prevent, and mitigate identity theft, says **Barbara Colburn,** director of operations for a medium-sized billing service in Wisconsin, and president of Total Health Care Solutions, a healthcare consulting firm in Wisconsin.

Updates: "If a report indicates that a program has serious flaws, it seems that the program should be revised to reduce risks of identity theft," Williams says. "If the report indicates that all is well, then there may not needto be any updates at that time."

You don't necessarily have to revise your program each time you revisit it, but "it seems likely that there will be some tweaks needed for any new program,"Williams says. "And, a program will not be effective unless it is updated to keep up with internal and external developments."

To read the FTC's advice about the rule, visit www.ftc.gov/bcp/edu/pubs/articles/art11.shtm.