# Eli's Rehab Report

## Regulations: Red Flags Rule Is Off The Table For Therapy

**But you shouldn't skimp on ID theft protections, experts warn.**

Therapists worried about the federal mandate to protect their clients from identify theft can breath a sigh of relief.

On Dec. 18, **President Obama** signed the Red Flag Rules Program Clarification Act, which changed the wording of who is considered a "creditor" in the government's eyes for Red Flags Rule purposes.

Good news: The clarification lets most home care providers -- including physical and occupational therapy practices and speech-language pathology and audiology practices -- off the hook for related identify theft protection requirements.

Previously, the Red Flags Rule defined a creditor as any entity that bills a customer after rendering services. The **Federal Trade Commission's** website noted earlier this year that creditors included "many doctor's offices, hospitals, and other health care providers." As creditors, providers had to comply with the FTC's Red Flags Rule, which required creditors to develop programs to address identity theft prevention techniques, as well as tools to detect and deal with potential identity theft incidents.

New ruling: The "Red Flag Clarification Act of 2010" signed by the president indicates that a true "creditor" meets the following criteria:

- Obtains or uses consumer reports in connection with credit transactions;
- Furnishes information to consumer reporting agencies; and
- Advances funds to or on behalf of a person that the person will pay back later.

Next step: Though the new clarification eliminates health care providers, many advocacy organizations want the FTC to specifically indicate in writing that providers are exempt from the Red Flags Rule.

**Take Advantage Of Your ID Protection Work**

Your practice is exempt from the Red Flags Rule, but that doesn't mean the work you've done tighten up your identity theft prevention processes was for nothing. The provisions in the Red Flags Rule are still considered smart if you want to avoid problems, says **James Hook,** director of consulting services with **The Fox Group,** a healthcare consulting firm based in Upland, Calif.

Reality: Your organization is still legally responsible for protecting the confidential information that patients give to you, Hook says. If you created a Red Flags program, don't just toss it aside -- instead, continue to implement the safeguards that you put in place to protect your patients.

And you should have processes in your organization to safeguard the information that patients have given to you. Often in a medical setting, "identity theft is, unfortunately, an inside job," Hook says. "Someone might take just enough information to use a patient's identity or even take their credit card information," he points out. There isn't much you can do to defend yourself against the dishonest actions of one employee acting alone, but you do want to have at least a bare minimum outline of what you'd do in the event that you found someone has misused patient information.

Don't forget: "Also, make sure you have a plan in place when you find someone seeking treatment with a stolen identity -- for instance, notifying the real patient and, potentially, law enforcement," Hook adds.

Resource: Read the clarification at www.gpo.gov/fdsys/pkg/BILLS-111s3987enr/pdf/BILLS-111s3987enr.pdf.

Codify
BY AAPC