SEYFARTH SHAW LLP
ATTORNEYS

One Minute Memo®

UPDATE

Is Your Health Care Institution Ready to Comply with New Regulations to Combat Identity Theft?

The FTC has once again delayed the enforcement of these new regulations from August 1, 2009 to November 1, 2009.

On April 30, 2009, the Federal Trade Commission (FTC) issued a press release that it would delay enforcement of the new regulations from May 1, 2009 to August 1, 2009. Additionally, the FTC has published a "template policy" on its website (www.ftc.gov/redflagsrule).

The new regulations were originally set to go into effect on November 1, 2008; however, on October 22, 2008, the FTC announced that it would suspend enforcement of the new regulations until May 1, 2009, granting additional time for affected creditors and financial institutions to develop and implement a written Identity Theft Prevention Plan.

The new regulations are designed to combat identity theft, and some of the requirements will likely apply to hospitals and other providers of medical care. The regulations, known as "Red Flag" rules, are designed to help uncover, prevent, or mitigate identity theft in different types of financial transactions. The section of the regulations that likely applies to hospitals and other health care institutions requires all "creditors" that hold consumer or other "covered accounts" to develop and implement a written identity theft prevention program that covers both new and existing accounts.

Why are health care institutions likely covered?

The definition of "creditor" under the regulations is broad enough to cover any hospital that defers payment for services rendered. "Covered accounts" include those accounts that are used for personal, family or household purposes and include multiple payments or transactions. Therefore, any payment for medical services other than a full, lump-sum cash payment made at the time service is rendered, is a covered account. This includes payment plans, deferred billing programs, and most submissions to insurance.

What do hospitals need to do?

Hospitals must develop and implement a written Identity Theft Prevention Plan that is designed to:

- **Identify suspicious activity or "red flags" that signal the possibility of identity theft in a covered transaction.**

Examples include (but are not limited to) fraud alerts by consumer reporting agencies, presentation of suspicious documents, inconsistencies among documentation already maintained by the hospital, and notices of alleged identity theft from consumers or law enforcement.

- **Detect a red flag when it actually arises.**
- **Implement a policy to effectively respond to a red flag and reduce the risk of further identity theft.** This may be as simple as confirming a change in address or name change, or may involve more in-depth analysis of suspicious activity.
- **Update the program periodically.**

Finally, hospitals are also required to have their boards of directors approve the program before it is put into place. While the new identity theft regulations are not complicated, they are detailed, and require covered entities to implement carefully considered policies and procedures.

For more information regarding these regulations, or for assistance in making sure your identity theft and background screening processes are compliant with state and federal law, contact your Seyfarth Shaw attorney or contact any Labor and Employment attorney on our website (www.seyfarth.com/LaborandEmployment).

SEYFARTH SHAW LLP
ATTORNEYS

Breadth. Depth. **Results.**

www.seyfarth.com