

CLIENT ALERT

SHERMAN SILVERSTEIN

ATTORNEYS AT LAW

RED FLAGS RULE

Author:

Thomas J. Tamburelli

Health Care Law Practice Group

856.661.2090

ttamburelli@shermansilverstein.com

Mr. Tamburelli is a shareholder at Sherman Silverstein, where he focuses on health care law and contracts.

4300 Haddonfield Road
Pennsauken, NJ 08109

T: 856.662.0700

F: 856.662.0165

shermansilverstein.com

Sherman Silverstein Client Alerts are published by Sherman, Silverstein, Kohl, Rose & Podolsky, P.A., as a service to clients and friends of the firm. The information contained in this publication should not be construed as legal advice. Please consult your attorney regarding specific situations. If you are not on the firm's mailing list and wish to subscribe to future client alerts and newsletters, please e-mail your contact information to info@shermansilverstein.com.

© 2009 Sherman, Silverstein, Kohl, Rose & Podolsky, P.A. All rights reserved.

HIPAA compliance.....*check*. Stark compliance.....*check*. Coding and billing compliance.....*check*. "Red Flags Rule" compliance.....?!!!!!!!

As if there isn't enough for physician practices and other health care providers to address, by August 1, they must also develop and implement a written "Identity Theft Prevention Program" under the "Red Flags Rule." The Rule is part of the Fair and Accurate Credit Transaction Act, and enforced by the Federal Trade Commission ("FTC"). The American Medical Association ("AMA") has challenged the application of the Rule to physicians and the health care industry. However, to date, we understand it has only been successful in delaying implementation until August 1. According to the AMA, the FTC "considers physicians who accept insurance or allow payment plans to be creditors, and therefore subject to the [Rule]."

Fortunately, the FTC and the AMA have provided helpful resources for physician practices to utilize in the development of their Identity Theft Prevention Program. Also, the FTC acknowledges that a business with a low risk of identity theft could develop a more streamlined Program.

According to the FTC, a "Program must include four basic elements [or steps], which together create a framework to address the threat of identity theft." The first step is to identify relevant "red flags" or warning signs of identity theft that you are likely to come across. (Categories of common red flags include: (a) alerts, notifications and warnings from a credit reporting company; (b) suspicious documents such as IDs that look altered or forged; (c) suspicious personal identifying information; (d) suspicious account activity; and (e) notices from other sources such as a victim of identity theft, law enforcement or others). The second step is to set up procedures designed to detect the identified red flags in day-to-day operations. The third step is to set forth actions that will be taken to prevent and mitigate the damage from identity theft. The fourth step is to keep the Program current and to educate staff.

If you would like assistance in the development of your Identity Theft Prevention Program, have questions about the applicability of the Rule to your practice or business or wish to have your Program reviewed by counsel, please let us know.

Contact:

Thomas J. Tamburelli
856.661.2090
ttamburelli@shermansilverstein.com