porterwright

Health Care Law Alert

A Corporate Department Publication

February 2009

Compliance Required: Identity Theft Red Flag Rules and Health Care Providers

Many health care providers do not realize that they must soon comply with new regulations designed to prevent consumer identity theft. Starting May 1, 2009, the Federal Trade Commission (FTC) will begin enforcing those regulations, known as the Red Flag rules. The FTC issued the rules as part of a joint rulemaking effort between the FTC and the federal bank regulatory agencies. Beyond financial institutions, the Red Flag rules apply to any business that "regularly extends credit." This broad definition encompasses many health care providers, requiring them to act quickly to comply with the upcoming May 1, 2009 deadline.

Despite an FTC opinion that specifically brings health care providers within the purview of the Red Flag rules if they otherwise qualify as creditors, many entities within the medical system — particularly physician practice groups — have yet to develop a program for compliance with the new rules. Indeed, they are hard pressed to fathom how their activities could possibly qualify them as creditors much less how their patients could be vulnerable to identity theft by virtue of their status as patients. To be sure, the risk of identity theft as a result of seeking medical care may be lower than other avenues of risk. That said, qualifying as a creditor under the Red Flag rules is as simple as offering patients the option of paying over time. Given the prevalence of that practice, many health care providers need to prepare for yet another layer of regulatory oversight.

The Red Flag rules require that each consumer creditor develop and implement a written identity theft prevention program for its covered accounts. A "consumer creditor" is defined as an entity that regularly extends, renews, or continues credit, arranges for such credit, or is assigned credit by the original creditor. "Covered accounts" include continuing credit relationships used for personal, family, or household purposes as well as any other accounts (including non-personal accounts) that have a reasonably foreseeable risk of identity theft. Because health care providers often arrange for payment over time and because patient accounts are for personal or family use, many health care providers will fall under the Red Flag rules and must, therefore, develop and implement a written identity theft prevention program.

Richard G. Terapak
614-227-4301
rterapak@porterwright.com

John P. Carney
614-227-2179
jcarney@porterwright.com

Theodore G. Fisher
614-227-2040
tfisher@porterwright.com

Jack J. Gravelle
614-227-2084
jgravelle@porterwright.com

Charles Y. Kidwell
937-449-6739
ckidwell@porterwright.com

Linda R. Minck
239-593-2967
lminck@porterwright.com

Kenneth K. Rathburn
614-227-2128
krathburn@porterwright.com

Donna M. Ruscitti
614-227-2192
druscitti@porterwright.com

Daniel W. Scharff
513-369-4208
dscharff@porterwright.com

Mark K. Velasco
937-449-6723
mvelasco@porterwright.com

Please see our other publications at www.porterwright.com/publications.

porterwright

Each health care provider's program will differ depending on the types of red flags that the provider may be in a position to detect. Despite the Red Flag rules' broad application, they also offer flexibility for compliance depending on size, practice, and the extent to which the nature of the provider's business allows for the detection of identity theft. At their core, the Red Flag rules require that written identity theft prevention programs accomplish the following four objectives:

1. Identify the red flags of identity theft for covered accounts and outline those red flags in the program;
2. Monitor for and detect the red flags outlined in the program when they occur;
3. Respond appropriately to any detected red flags and mitigate identity theft; and
4. Ensure that the program is updated periodically to reflect changes in the risks presented to customers or other creditors from identity theft.

In light of these objectives, health care providers should consider the types of covered accounts they offer and how they establish and provide access to such accounts. For providers who have experienced data breaches or identity thefts in the past, the first step may simply be to update procedures already in place for protecting patients, such as procedures for HIPAA compliance. For smaller providers, a program may be as simple as developing ways to document and investigate unusual uses of covered accounts or suspicious changes to the personal information of account holders. In every case, staff must be trained to implement the program, and the directors and management will be responsible for oversight and reviewing compliance reports.

The FTC has identified 26 possible red flags that may be incorporated into a program if applicable. The red flags fall into several categories including suspicious documents, personal identifying information, account activity, and notifications regarding identity theft from customers, law enforcement, or a consumer reporting agency. One common red flag that is relevant for a variety of businesses is a material change in a customer's use of credit. In the health care area, this red flag may equate to an increased use of credit for medical devices or supplies. Similarly, depending on the practice, an increase in requests for prescription refills may signal possible identity theft. Other possible scenarios are sure to surface as identity thieves become more sophisticated.

Although the need for or scope of the Red Flag rules may be open for debate, the rules' effective date is not. Health care providers must move quickly as it will take time to develop, adopt, and implement a written identity theft prevention program and adequately train all staff. All businesses subject to the Red Flag rules, including health care providers, will risk both civil monetary penalties and increased liability if they fail to comply.

Porter Wright Morris & Arthur LLP
www.porterwright.com

Cincinnati, Ohio
800-582-5813
Cleveland, Ohio
800-824-1980
Columbus, Ohio
800-533-2794
Dayton, Ohio
800-533-4434
Naples, Florida
800-876-7962
Washington, DC
800-456-7962