PUBLICATION

November 1 Deadline for Medical Identity Theft Prevention Programs and Address Discrepancy Requirement

October 10, 2008

Beginning on November 1, 2008, businesses that extend or arrange credit for customers will be required to have written identity theft prevention programs. In the case of creditors in the health care field, risk of medical identity theft, that is, identity theft for the purpose of obtaining medical services, must also be addressed. The programs, whether for identity theft prevention generally or medical identity theft prevention specifically, must meet the requirements of regulations issued by the Federal Trade Commission under the so-called "Red Flags Rule." A key element of the Red Flags Rule is that boards of directors and senior managers must have oversight responsibility for their organizations' identity theft prevention programs.

The Red Flags Rule is meant to apply to those who regularly extend or arrange for credit and assignees of original creditors. This definition includes finance companies and non-profit and government entities when they defer payment for goods or services. Organizations that merely accept credit cards as forms of payment are not deemed to be "creditors" under the Red Flags Rule.

Even if an organization is a "creditor," the Red Flags Rule only applies to its "covered accounts." These are accounts that are used mostly for personal, family or household purposes, and that involve multiple payments or transactions. However, certain business accounts are also included as covered accounts. "Covered accounts" also include any other account that the creditor offers or maintains for which there is a reasonably foreseeable risk of identity theft.

With regard to health care providers, if a provider extends credit to a patient by establishing an account that permits multiple payments, the provider is a creditor offering a covered account and is therefore required to comply with the Red Flags Rule. Creditors must have in place identity theft prevention programs that have four basic elements:

1. ***Identification of relevant red flags*** - The five categories of red flags that a program must identify and address, as applicable, are:

Alerts, notifications, or warnings from a consumer reporting agency;

Suspicious documents such as an ID that looks altered;

Suspicious personally identifying information such as a lack of correlation between the SSN range and the date of birth of an individual;

Suspicious activity relating to a covered account such as notice of a change of address for an account quickly followed by a request for the addition of new authorized users on the account; or

Notices from customers, victims of identity theft, law enforcement authorities, or other entities about possible identity theft in connection with covered accounts.

2. ***Detection of red flags*** - The program should detect red flags through, among other things, authentication of customers, monitoring transactions, and verification of change of address requests.
3. ***Prevention and mitigation of identity theft*** – Program policies and procedures should include appropriate responses to red flags in the context of the risk. As an example, if there has been an unauthorized access to a customer account, appropriate responses might include monitoring the account, changing passwords or closing the account.
4. ***Periodic updating of the program*** – A program should be updated and reviewed periodically based on factors such as changes in identity theft methods, changes in covered accounts offered or an incidence of identity theft suffered by the organization.

When identifying the red flags, a creditor should take a risk-based approach in the context of the types of accounts it has, methods it uses to open and access accounts and its prior experiences with identity theft. Health care providers, who are required to comply with the HIPAA Security Rule, should be familiar with this approach and be able to roll the Red Flags Rule identity theft prevention plan requirements, commencing with a risk assessment, into their HIPAA plans. As is the case with HIPAA, the red flags requirements are in the context of the organization being assessed. The complexity and depth and breadth of an identity theft prevention plan of a small provider practice certainly need not be the same as that of a large, national hospital owner.

Identity theft is a growth industry with, according to a Gartner study, a 2006 victim population of 15 million. Medical identity theft, which has the added dimension of potential bodily harm, death or depletion of insurance benefits, is a particularly pernicious version of the crime. The costs of identity theft to victims and businesses are very high and government regulators are increasingly enforcing current laws and regulations, such as HIPAA, and implementing new ones.