Red Flag Rules Delayed

HEALTHCARE PROVIDERS HAVE ADDITIONAL TIME FOR COMPLIANCE

Healthcare Practice Group

Healthcare Alert

This Alert provides a brief overview of the Red Flag Rules and basic steps that providers need to take to have an identity theft program in place on May 1, 2009. As explained below, providers will need to perform an assessment of the application of the Red Flag Rules, develop written policies and procedures and implement an administrative framework in order to comply. This Alert also discusses the requirements applicable to users of consumer reports, which were not delayed.

Background

The FTC issued regulations in November 2007 directing "creditors" to implement programs designed to deter, detect and mitigate identity theft. The rules are commonly known as the "Red Flag Rules" because creditors must look for suspicious "red flags" that could signal the presence of identity theft. The FTC has construed the term "creditors" broadly as businesses that provide services or supplies without requiring upfront payment. Therefore, although a healthcare provider is not a creditor in the traditional sense, a healthcare provider that bills the patient and/or the patient's insurer after services are delivered is a creditor and the Red Flag Rules apply.

Identity Theft Program

The Red Flag Rules do not dictate specific requirements for identity theft programs, but only direct that a creditor establish reasonable policies and procedures in its program. To create these policies, a provider must determine the kinds of information it collects and maintains that are susceptible to identity theft. For example, providers may use demographic information that is contained in both paper and electronic formats in medical charts, files used to verify insurance coverage and patient billing records. A provider may have policies already in place that address these issues in whole or in part, such as patient registration policies that request certain identification information or procedures to verify coverage with insurers.

Next, a provider must determine what patterns, practices or activities related to this information could be signs of identity theft. Possible red flags include forged forms of identification or insurance cards, suspicious address changes or receipt of information that does not match information already on file. The provider must then develop policies that explain how it will respond to potential issues detected. Appropriate responses may include contacting the patient's insurer, investigating address changes, and noting discrepancies in the patient's chart and files.

The Red Flag Rules impose administrative requirements related to the identity theft program. These include obtaining board approval of the program, assigning responsibility for its operation, making annual reports regarding compliance, periodically updating the program and training staff about its application. The Red Flag Rules also require providers to ensure that service providers that perform duties related to information subject to identity theft implement reasonable policies to detect, deter and mitigate the risk of identity theft.

Use of Consumer Reports

As noted above, the FTC did not delay the requirements related to the use of consumer reports. Healthcare providers may request consumer credit reports with respect to patients or applicants for employment or medical staff appointment as part of the screening process. The Red Flag Rules require parties which use consumer credit reports to have procedures in effect to permit them to assess situations in which the address on a report does not match the address given by the patient or applicant and in certain instances would require that the provider report address information to a consumer reporting agency.