



# Adelman, Sheff & Smith LLC

180 ADMIRAL COCHRANE DRIVE | SUITE 370 | ANNAPOLIS | MARYLAND | 21401 | TEL. (410) 224-3000 | FAX. (410) 224-0098  
200-A MONROE STREET | SUITE 310 | ROCKVILLE | MARYLAND | 20850 | TEL. (301) 340-1140 | FAX. (301) 294-6406

**October 10, 2008**

**► CLIENT ALERT ◀**

## **Compliance with FTC's Identity Theft Red Flag Regulations – Upcoming November 1, 2008 Compliance Deadline**

Last year, the Federal Trade Commission (FTC) issued new regulations called the Red Flag rules aimed at preventing, detecting, and deterring identity theft. The term “Red Flag” comes from the FTC requirement that businesses identify “red flags” that might indicate an attempt at identity theft such as presentation of questionable identification. Given the breadth of these regulations, the Red Flag rules may have implications for health care providers regardless of whether they are for profit, non-profit, or government entities. Under the Red Flag rules, financial institutions and creditors (broadly defined to potentially encompass health care institutions and providers) of “covered accounts” (discussed below) must establish a formal program to detect, deter, and mitigate identity theft with an upcoming compliance date of November 1, 2008.

Although the FTC has not issued any formal statements confirming that the Red Flag Rules apply to health care providers, during a recent teleconference with an advisory attorney from the FTC, the attorney stated that the Red Flag Rules did apply to health care providers. Without additional guidance or a ruling from the FTC, it is prudent for health care providers to assume they will be subject to the Red Flag rules and therefore, make plans to comply with them. As such, hospitals are well advised, either through their existing HIPAA privacy and security rule policies and procedures or through the creation of new Red Flag Rules policies and procedures, to protect patients from medical identity theft.

Applicability of the Red Flag rules turns on two key defined terms. First, a creditor is broadly defined to include any person or entity that “regularly extends, renews, or continues credit.” In the health care context, FTC staff members have indicated that they consider the deferring of payment obligations for medical services rendered to be extending credit. By way of example, according to an FTC advisory attorney, if a patient pays a co-pay at the time of service but the health care provider does not collect full payment in anticipation of billing the patient’s health insurance, the hospital would be considered to be extending credit.

Second, under the Red Flag rules, a covered account is defined broadly as:

- 1) an account maintained primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions; and



- 2) any other account for which there is a reasonably foreseeable risk to customers, or to the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation or litigation risk.

Patient accounts would seem to fall under both prongs of the definition of a covered account since hospitals often allow patients to pay medical bills over time with multiple payments. Supplementary information in the final Red Flag rule states: "For instance, creditors in the health care field may be at risk of medical identity theft (i.e., identity theft for purpose of obtaining medical services) and, therefore, must identify Red Flags that reflect this risk."

## **Ensuring Compliance with the Red Flag Rules**

If a health care institution or provider falls under the Red Flag rules, they must develop and implement a written identity theft prevention program that is tailored to match the size, complexity, and nature and scope of the business conducted – allowing for some flexibility in the design of the program. The Red Flag rules require that the program include reasonable policies and procedures to accomplish the following:

- **Identify Red Flags** – relevant patterns, practices, and specific activities that signal possible identity theft. Included as an appendix to the regulations is a listing of potential red flags, including suspicious documents, suspicious personal information, unusual activity, and inquires or notice from potential victims of identity theft. In addition, the World Privacy Foundation and others have issued annotated lists of Red Flags specifically geared to health care providers that are particularly useful:
  - **Complaint or question from a patient related to a patient's receipt of a bill for another individual; a bill or explanation of benefits for a product or service the patient claims he or she did not receive; or a bill from a provider the patient was not seen by;**
  - **Records indicating medical treatment that is inconsistent with the patient's physician examination or medical history;**
  - **Complaint or question from the patient concerning collection activities;**
  - **Notification from the patient or insurance company of denial of coverage due to exhaustion of benefits or that the patient has reached his or her benefit cap;**



- **Complaint or question from a patient concerning the patient's credit report and the inclusion of a health care provider or insurer;**
  - **Any dispute by a patient concerning the validity of a bill for services and potential identity theft;**
  - **Presentation of documents that appear forged, altered, or fake;**
  - **Suspicious change of address requests;**
  - **Failure of a patient to produce an insurance card or other documentation of insurance where the patient has an insurance number; and**
  - **Any notice or inquiry from an investigator, private insurance company, or law enforcement agency.**
- **Detect Red Flags** – Providers should have processes in place to appropriately detect red flags once the program has been implemented. Such processes may include patient authentication (require the patient to produce identifying information at the time the account is opened and upon receiving services), monitoring of transactions, and validating any change of address requests.
  - **Respond Appropriately to Red Flags** – Hospital's policies should contain an identity theft mitigation strategy that may include the following: monitoring covered accounts, contacting patients when questions arise or suspicious activity is detected, changing passwords or security codes, notifying law enforcement when appropriate, and addressing documentation issues in the patient's medical record that may be related to identity theft (ensuring the medical record is accurate). For example, if an inquiry is made about services provided, an appropriate response would be to contact the provider of the services and verify that the services were provided and obtain additional information or if there is a discrepancy with the address to ask for additional information. From a compliance perspective, any response to detected red flags should be documented.
  - **Update the Program Periodically** – to reflect any perceived or real changes in the risk of identity theft in your organization.



In addition to the policies and procedures, the Red Flag rules include the following with respect to the administration of the identity theft program:

- **Obtain Written Board Approval** – the identity theft program must be approved by the Board of Directors or an appropriate committee of the Board of Directors;
- **Designation of Oversight Responsibilities** – the Board or an individual of senior level management must be involved in the oversight, development, management, and administration of the program;
- **Training and Compliance Monitoring** – staff must be trained to allow for the implementation of the program, including through increased awareness of the risk of identity theft and how it impacts victims. Oversight and compliance with the program should be monitored.

## **Penalties for Non-Compliance**

The FTC's plan with respect to monitoring compliance with the Red Flag rules is not clear. Nevertheless, failure to comply with the Red Flag rules could result in the imposition of monetary penalties. The FTC is authorized to bring enforcement actions in federal court for violations with penalties set at \$2,500 per independent violation. State enforcement action is authorized on behalf of victims with penalties set at \$1,000 per violation and reasonable attorney fees. Finally each patient may be entitled to bring a civil action and recover actual damages sustained from a violation of the Red Flag rules.

## **Conclusion**

Although the Red Flag rules present yet another set of compliance issues for health care providers and organizations, even if the rules are ultimately determined not to apply to hospitals or health care providers, taking steps to detect and prevent identity theft is still a good idea. Accordingly, the more prudent and responsible course is probably for healthcare providers to comply with the rules. The deadline for compliance with the Red Flag rules, which includes Board approval, is November 1, 2008. If you have any questions or if we can be of any assistance to you in developing policies or procedures to address the Red Flag Rules, or to deal with identity theft, please do not hesitate to contact us.

**For more information, please contact:** **Cathy Martin 410-224-3000 [cmartin@hospitalaw.com](mailto:cmartin@hospitalaw.com)**  
**Tim Adelman 410-224-3000 [tadelman@hospitalaw.com](mailto:tadelman@hospitalaw.com)**

*This Client Alert was prepared as a service to our clients. The information discussed is general in nature and may not apply to your specific situation. Legal advice should be sought before taking action based on the information contained in this Client Alert.*