

MEMORANDUM

CLIENT-MATTER NUMBER
999700-0712

TO: American Ambulance Association Members

FROM: R. Michael Scarano, Jr.

DATE: March 30, 2009

RE: Resources for Complying with "Red Flags Rules"

Effective May 1, 2009, the so-called "Red Flags Rules" ("Rules") require that most ambulance service providers ("providers") have in place a written program ("Program") to prevent, detect and mitigate identity theft. The Rules went into effect January 1, 2008, with an initial mandatory compliance date of November 1, 2008. However, on October 22, 2008, the Federal Trade Commission ("FTC"), the primary agency responsible for enforcing the Rules, delayed enforcement until May 1, 2009, citing confusion and uncertainty within major industries about the applicability of the Rules.

The Rules were enacted pursuant to the Fair and Accurate Credit Transactions Act of 2003, which was directed primarily at financial institutions and other creditor agencies. However, the Rules apply broadly to any organization, including ambulance services and other health care organizations, which meet the definition of a "creditor" and that offer or maintain "covered accounts." These terms are defined broadly enough to cover most ambulance providers, including governmental and nonprofit services which bill for their services. The FTC has clarified that a health care provider is deemed a "creditor" under the Rules if it regularly extends, renews or continues credit. Under the Rules, "credit" means an arrangement by which an organization defers payment of debts or accepts deferred payments for the purchase of property or services. In other words, if an organization permits payment to be made after the product is sold or the service is rendered, the organization is deemed to be a "creditor".

The FTC has said:

“Health care providers are creditors if they bill consumers after their services are completed. Health care providers that accept insurance are considered creditors if the consumer ultimately is responsible for the medical fees.”¹

The Rules focus on identifying and responding to “Red Flags”. A Red Flag is defined as “a pattern, practice or specific activity that indicates the possible existence of identity theft.” In other words, a Red Flag is a warning sign regarding the possibility of identity theft.

The Rules are found at 16 CFR § 681.2, and are supplemented by Guidelines found in Appendix A to 16 CFR Part 681, and a Supplement to the Guidelines. These materials are attached as Exhibit A to this memorandum. Also attached are an example of a Policy/Procedure establishing a Program and a Resolution of the Board of Directors approving the Program. The following summarizes the requirements of the Rules.

Risk Assessment

Although most providers are clearly covered by the Rules, the Rules require that each organization meeting the definition of “creditor” determine, at the inception of its Program and periodically thereafter, whether it offers or maintains “covered accounts.” A “covered account” is defined as: (1) an account that the provider offers or maintains primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions; and (2) any other account that a provider offers or maintains for which there is a reasonably foreseeable risk of identity theft. This definition would include most (if not all) of the providers’ accounts for individual patients, and could include some of its business accounts if they present a reasonably foreseeable risk of identity theft.

In determining whether they maintain covered accounts, providers must conduct a risk assessment to determine whether their covered accounts present a reasonably foreseeable risk of identity theft. The risk assessment must take into consideration: the methods the provider uses to open its accounts; the methods it provides to access its accounts; and its previous experiences with identity theft. Section II of the Policy addresses the required Risk Assessment.

Establishment of an Identity Theft Prevention Program

Each creditor that offers or maintains one or more covered accounts must develop and implement a written Program that is designed to detect, prevent and mitigate identity theft in connection with opening or maintaining such accounts. The Rules require creditors to perform the following four functions in their Programs:

¹ The Red Flags Rule: What health care providers need to know about complying with new requirements for fighting identity theft. www.FTC.gov/bcp/edu/pubs/articles/art111.shtm.

- identify Red Flags relevant to the organization's accounts;
- establish procedures for detecting Red Flags;
- establish procedures to prevent and mitigate identity theft when Red Flags are detected; and
- update the Program periodically.

The following describes each of these required functions.

Identify Relevant Red Flags

A provider's written Program must identify the Red Flags (i.e., warning signs) indicating the possibility of identity theft. The Guidelines provide that a creditor should consider the following factors in identifying relevant Red Flags: the types of covered accounts that it offers or maintains; the methods it provides to open its covered accounts; the methods it provides to access its covered accounts; and its previous experiences with identity theft. The Rules further instruct creditors to incorporate relevant Red Flags from sources such as incidents of identity theft the creditor has experienced; methods of identity theft the creditor has identified that reflect changes in identity theft risks; and applicable regulatory guidance.

The Program should include relevant Red Flags from five categories specified in the Rules:

- alerts, notifications or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
- the presentation of suspicious documents;
- the presentation of suspicious personal identifying information, such as a suspicious address change;
- the unusual use of, or other suspicious activity related to, a covered account; and
- notices from consumers, victims of identity theft, law enforcement authorities or other persons regarding possible identity theft in connection with covered accounts.

Detailed examples of Red Flags from each of these categories are found in the Supplement to the Guidelines. Some specific potential Red Flags applicable to health care providers, some of which are not included in the Rules, include situations involving the exhaustion of lifetime benefits; denials for duplicate or excessive services for an individual; reports by an individual that he or she received a bill or an explanation of benefits for a transport or other medical services that the individual claims he or she did not receive; discrepancies in information collected at the time of providing patient care services (e.g., the name on an insurance card not matching the name on the individual's driver's license). Section III of the attached Policy addresses this part of the Program.

Detect Red Flags

Once a creditor has identified the Red Flags that are relevant to its business, its policies should address the detection of those Red Flags in connection with the opening of covered accounts and the maintenance of existing accounts. For example, the creditor may establish procedures for obtaining identifying information about, and verifying the identity of, persons to whom services are provided. In the ambulance context, this could involve requesting government issued identification such as a driver's license or Medicare card at the time of service, provided this can be performed without jeopardizing patient care. Emergent or urgently needed care should never be delayed to obtain identification. In the ambulance context, it will frequently not be possible to check identity in advance of the transport. A provider's business office may also spot Red Flags when it verifies a patient's identity, authenticates insurance information, or reviews medical records in preparing claims. This function is addressed in Section IV of the Policy.

Preventing and Mitigating Identity Theft

A provider's Program must include appropriate responses to Red Flags, when detected, commensurate with the degree of risk posed by the Red Flag. In determining an appropriate response, the provider should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to patients' accounts, or notice that a patient has provided information related to a covered account to someone fraudulently claiming to represent the organization. The Rules set forth some examples of appropriate responses. These include, without limitation, monitoring accounts; contacting the patient; reopening a covered account with a new account number; not opening a new covered account; closing an existing covered account; notifying law enforcement; or determining that no response is warranted under the particular circumstances. This function is addressed in Section V of the Policy.

Update the Program Periodically

The Rules require creditors to update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in identity theft risks to its patients or to the safety of the creditor from identity theft. In performing such updates, the creditor should consider factors such as: the experiences of the organization with identity theft; changes in methods of identity theft; changes in methods to detect, prevent and mitigate identity theft; changes in the types of accounts that the organization offers or maintains; and changes in business arrangements of the organization, including but not limited to changes in its relationships with service providers. The annual update function is addressed in Section VIII of the Policy.

Methods for Administering the Program

The Rules require creditors to provide for the continued administration of the Program by taking certain steps. These include:

- obtaining approval of the initial written Program from either the creditor's board of directors or an appropriate committee of the board (or, if the provider does not have a board or other governing body, by a senior management employee);
- training staff, as necessary, to effectively implement the Program; and
- involving the board, the designated committee or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program.

The oversight function specified in the Rules should include: assigning specific responsibility for the Program's implementation; reviewing reports prepared by staff regarding compliance by the creditor with the Rules; and approving material changes to the Program, as necessary to address changing identity theft risks. The reports prepared by staff should address material matters related to the Program, and evaluate issues such as the effectiveness of the Program in addressing the risk of identity theft; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.

Finally, administration of the Program should include oversight of service provider arrangements. The creditor must take steps to insure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft. For example, the creditor could require the service provider to contractually agree to implement its own Red Flags policies, and to either report the Red Flags to the creditor, or take appropriate steps to prevent or mitigate identity theft itself. Providers should consider amending either their service agreements or their business associate agreements with their service providers to require them to comply with these obligations.

Sample Policy/Procedure for Identity Theft Program

Attached to this memorandum as Exhibit B is a Sample Policy/Procedure for Identity Theft Identity Prevention, Detection and Mitigation Program ("Sample Policy"), designed for an ambulance service. The Sample Policy is not intended as a substitute for a provider performing its own risk assessment, as required by the Rules, and crafting a Program based on its own unique circumstances. Each provider should review the Rules, including the Guidelines and the Supplement to the Guidelines, prior to establishing its own Program and policies. The Sample Policy is intended as a starting point for undertaking that process. Also attached as Exhibit C is an example of a Board Resolution that can be used in approving a provider's Program. If the organization does not have a board or other governing body, the program can be approved by an employee at the level of senior management.