SHUMAKER
Shumaker, Loop & Kendrick, LLP

October 20, 2008

Health Law Client Action Letter

FTC Red Flags Rules Require Many Healthcare Providers to Adopt an Identity Theft Program by November 1, 2008

The Federal Trade Commission ("FTC"), in conjunction with other agencies, recently issued regulations requiring financial institutions and creditors to have a written identity theft program in place by November 1, 2008. The program must include reasonable policies and procedures designed to detect, prevent, and mitigate identity theft in connection with certain accounts, and must address "Red Flags," defined as any "pattern, practice, or specific activity that indicates the possible existence of identity theft." (For this reason, the regulations are referred to as the "Red Flags Rules.") "Identity theft" means "a fraud committed or attempted using the identifying information of another person without authority." Healthcare organizations and physician groups subject to the Rules must implement an identity theft program by the November 1 deadline.

Healthcare Organizations and Physician Groups as "Creditors." "Financial institutions" and "creditors" that offer or maintain "covered accounts" are subject to the Red Flags Rules. The term "creditor" includes any party that regularly defers payment for services rendered. Because many healthcare organizations arrange for payment over time for services previously rendered, their billing practices would qualify them as creditors. The FTC has also taken the position that physicians can be creditors. The American Medical Association and others have questioned this interpretation and have asked the FTC to reconsider its view that the Rules should apply to physicians. They have also asked the FTC to delay any plans to apply the Rules to physicians until it reviews and responds to this request. However, the Rules are effective as to physician creditors on November 1, 2008 unless the FTC acts to delay this date.

Offering or Maintaining "Covered Accounts." The Red Flags Rules require a creditor to implement an identity theft program in connection with the "opening of a covered account or any existing covered account." The Rules define a "covered account" as either: (1) "an account that a ... creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transaction;" or (2) "any other account that the ... creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft." Accounts offered or maintained by a healthcare organization that extend credit to a patient by allowing multiple payments are "covered accounts" under the first definition. Patient records that contain sensitive personal information—e.g. financial or medical—are "covered accounts" under the second definition if maintained by a "creditor."

Developing a Compliant Program. The regulations set forth guidelines on how healthcare organizations qualifying as creditors offering or maintaining covered accounts are to develop and administer their identity theft programs. The program must be written, and it must enable the healthcare organization to identify, detect, and respond appropriately to relevant Red Flags from

five separate categories, and to ensure the program is updated periodically to reflect changes in identity theft risks. **A healthcare organization's governing body (typically the board of directors) or an appropriate committee must approve the initial written program.** The board of directors, an appropriate committee, or a designated senior management-level employee must be involved in its oversight, development, and administration. The regulations allow for flexibility in developing a program that is appropriate to the size, complexity, and nature of the healthcare organization. Incorporation of existing policies, such as HIPAA Privacy and Security policies, is allowed and may facilitate implementation of the program.

Penalties for Violating the Red Flags Rules. The FTC is charged with enforcing the Red Flags Rules and it may impose a civil penalty of not more than $2,500.00 per violation for certain knowing violations of the Rules. Violators may also face individual state actions for injunctions or for damages on behalf of residents. Users of "consumer reports" may face other civil liability as well. "Consumer reports" include communications by a consumer reporting agency bearing on a consumer's credit, character, reputation, personal characteristics, or mode of living which are used as a factor in establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes.

If your organization is a creditor under the Rules but does not currently hold covered accounts, it must perform periodic determinations as to whether it offers or maintains such accounts. The Red Flags Rules contain other provisions that may affect whether an organization is subject to its requirements and the development and administration of an identity theft program. The above summarizes the key aspects of the Rules, but is not intended to be complete.

* * * * * * * *

If you have any questions concerning this newsletter, please call Dennis Witherell, Jenifer Belt, or Karl Strauss at 800-444-6659.

This newsletter is designed to provide general information on matters of interest to health care providers and practitioners and is not intended to constitute legal advice.