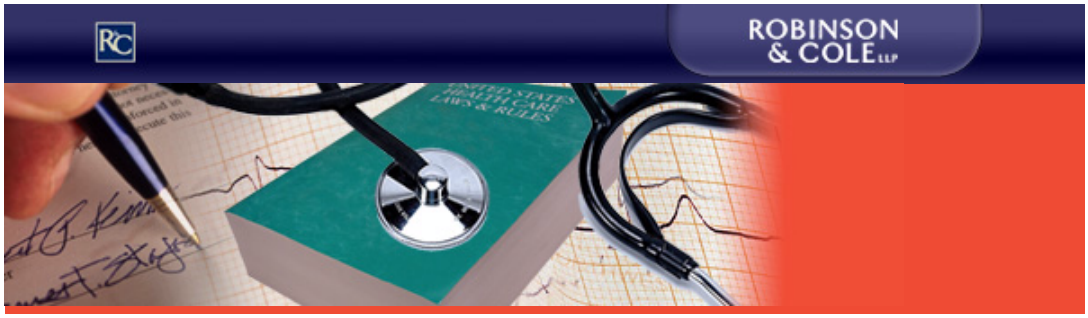

ATTORNEY ADVERTISING

OCTOBER 2008

Health Care Entities that Extend Credit to Patients Must Implement an Identity Theft Prevention Program

Health care entities that do not require their patients to fully pay for health care services on the date such services are rendered may need to comply with the Federal Trade Commission's red flag rules (the "Red Flag Rules"). As of November 1, 2008, all health care entities that qualify as creditors and maintain certain covered accounts must have a written identity theft prevention program that detects, prevents and mitigates identity theft (the "Program"). A summary of the Red Flag Rules and Program requirements is provided below.

Applicability

In order to determine whether your health care entity needs to comply with the Red Flag Rules, you need to first determine whether it qualifies as a creditor. A "creditor" is any person who regularly extends, renews, or continues credit or regularly arranges for the extension of credit for services rendered. As such, if your health care entity enters debt relationships with its patients by permitting such patients to defer payment (beyond the date of service) for health care services rendered, then such entity would likely qualify as a creditor.

Second, if you determine that your health care entity qualifies as a creditor, you must then determine whether it maintains covered accounts. "Covered accounts" are accounts that (i) are created primarily for personal or family purposes (i.e., receipt of health care services) and that can be paid off over multiple payments, or (ii) have a reasonably foreseeable risk to customers or to the safety and soundness of the health care entity from identity theft. As such, if your health care entity maintains accounts for its patients and such patients are permitted to pay the balance of those accounts over multiple payments, and/or your health care entity maintains accounts that have a reasonably foreseeable risk of identity theft, then such accounts would qualify as covered accounts. Most typical patient accounts qualify as covered accounts under both prongs of the "covered accounts" definition.

In light of the foregoing, if your health care entity qualifies as a creditor and maintains covered accounts (a "Covered Entity"), then it must implement a Program.

Program Requirements

While a Covered Entity has flexibility in implementing a Program that is appropriate to its size, complexity, and nature and scope of its activities, it must satisfy various requirements to fully comply with the Red Flag Rules. First, a Program must include policies and procedures that:

- Identify relevant patterns, practices, or specific activities that indicate the possible existence of identity theft ("Red Flags") by auditing the covered accounts that the health care entity offers or maintains;
- Incorporate any identified Red Flags into its Program;
- Detect Red Flags that have been incorporated into its Program;
- Respond appropriately to any Red Flags that are detected in order to prevent and mitigate identity theft; and
- Ensure the Program (including the Red Flags determined to be relevant) is updated periodically to reflect changes in risks to customers and to the health care entity's

safety and soundness from identity theft.

Second, in addition to implementing the foregoing policies and procedures, a Covered Entity must:

- Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;
- Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;
- Train staff, as necessary, to effectively implement the Program; and
- Exercise appropriate and effective oversight of service provider arrangements to ensure that such service providers are also complying with the Red Flag Rules.

Lastly, the Red Flag Rules provide that a Covered Entity must review a lengthy list of federal guidelines and include in its Program those guidelines that are appropriate for the Program. Such guidelines are available by clicking here.

Notwithstanding the foregoing, many of the Red Flag Rules' requirements overlap with the privacy and security requirements under the Health Insurance Portability and Accountability Act ("HIPAA"). As such, you might want to review your health care entity's HIPAA compliance efforts and determine whether some of such efforts may be duplicated into your Program.

Determining whether the Red Flag Rules apply to your health care entity requires a fact specific analysis. If you have any questions as to whether your health care entity qualifies as a creditor and maintains covered accounts, or need assistance with creating an identity theft prevention program that complies with the Red Flag Rules, please contact any member of Robinson & Cole's Health Law Group.

Robinson & Cole's Health Law Group includes:

Lisa Boyle
Theodore J. Tucci
Karen P. Conway
Michael J. Kolosky
B. Moses Vargas
Brian D. Nichols
Susan E. Roberts
Kimberly Troland

For more information, please contact Lisa Boyle at lboyle@rc.com or 800-826-3579.

The information in this update should not be considered legal advice. Consult your attorney before acting on anything contained herein.