



Beyond HIPAA: FTC Red Flag Rules and Health Care Providers

Kelli F. Robinson

Although covered by a multitude of federal and state regulatory agencies, most health care providers do not typically consider themselves regulated by the Federal Trade Commission (FTC). However, the FTC has recently interpreted its “Red Flag Rules,” which require the implementation of a program to detect and mitigate the effects of identity theft, as applying to the health care sector. Medical identity theft can occur when someone uses another person’s name and sometimes other parts of their identity, such as insurance information or Social Security Number, without knowledge or consent, to obtain medical services or goods.

Accordingly, health care providers must implement an Identity Theft Protection Program, as required in the FTC Red Flag Rules, prior to May 1, 2009, or risk hefty FTC fines and potential private lawsuits should their patients become victims of identity theft.

What health care providers are covered?

While primarily aimed at financial institutions, the FTC Red Flag Rules also apply to any “creditor” that maintains any “covered accounts.” The FTC has now confirmed that any health care provider (whether for-profit or non-profit) that defers payment for goods or services, such as billing in arrears for medical treatment, is now subject to its Red Flag Rules. Because vast differences among payors and reimbursement plans cause a patient’s liability to be unknown at the time of the medical service, most health care providers – including hospitals, physicians, ambulatory surgery centers and others – will be deemed “creditors”

subject to the FTC Red Flag Rules as a result of the current health care insurance and payment systems. A “covered account” is 1) an account primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions; or 2) any other account for which there is a reasonably foreseeable risk to customers from identity theft.

What constitutes a Red Flag?

The following are examples of red flags that might arise in a health care context:

- A complaint or question from a patient based on the patient’s receipt of: a bill for another individual; a bill for a product or service that the patient denies receiving; a bill from a health care provider that the patient never patronized; a notice of insurance benefits for health services never received.
- Records showing medical treatment that is inconsistent with the physical examination or a medical history as reported by the patient.
- A dispute of a bill by a patient who claims to be the victim of any type of identity theft.
- A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance.
- A patient who produces an insurance card but fails to produce valid photo identification.

(Continued on page 8)

Beyond HIPAA: FTC Red Flag Rules and Health Care Providers



What do FTC Red Flag Rules require?

Prior to May 1, 2009, covered health care providers must develop an Identity Theft Protection Program (the Program) that is approved by the provider's governing body and implemented, and must train all appropriate staff on the Program. The FTC Red Flag Rules provide considerable flexibility, allowing entities to establish programs that are appropriate given their size and complexity and the nature and scope of their activities.

The Program must include policies and procedures that:

- Identify** relevant patterns, practices and specific forms of activities that are Red Flags signaling possible identity theft and incorporate them into the Program;
- Detect** those Red Flags;
- Respond** to detected Red Flags in order to prevent and mitigate identity theft; and
- Update** the Program to reflect changes in risks from identity theft.

It should not be overly burdensome for providers who are subject to the FTC Red Flag Rules to develop appropriate policies and procedures, particularly in view of the flexible approach taken by the rules. Because there is some natural overlap between the FTC Red Flag Rules and the Health Insurance Portability and Accountability Act (HIPAA), health care providers should immediately confer with their health care counsel to assess the potential areas of their medical practice that may be susceptible to identity theft,

and to discuss ways to specifically revise their HIPAA Compliance Plan to include the FTC Red Flag Rules.

Health Care Consulting Group

Lenora W. Pate 2311 Highland Avenue South Birmingham, Ala. 35242 205.930.5162 lpate@sirote.com	Joe Bluestein 2311 Highland Avenue South Birmingham, Ala. 35242 205.930.5123 jbluestein@sirote.com
--	--

Cynthia Ransburg-Brown 2311 Highland Avenue South Birmingham, Ala. 35242 205.930.5389 crbrown@sirote.com	Joseph T. Ritchey 2311 Highland Avenue South Birmingham, Ala. 35242 205.930.5292 jritchey@sirote.com
--	--

Kelli F. Robinson 2311 Highland Avenue South Birmingham, Ala. 35242 205.930.5158 krobinson@sirote.com	Ronald A. Levitt 2311 Highland Avenue South Birmingham, Ala. 35242 205.930.5274 rlevitt@sirote.com
---	--

Fred Coffey 305 Church Street, Suite 800 Huntsville, Ala. 35801 256.518.3612 fcoffey@sirote.com	Bradley J. Sklar 2311 Highland Avenue South Birmingham, Ala. 35242 205.930.5152 bsklar@sirote.com
---	---

Shirley M. Justice
One St. Louis Centre, Suite 100
Mobile, Ala. 36602
251.434.0108
sjjustice@sirote.com



Kelli F. Robinson practices in the areas of health care law and litigation. She received her B.S. degree in Business and Public Administration from Louisiana State University in 1989 and her J.D. degree from the Cumberland School of Law. Kelli has 12 years of corporate human resources experience with such companies as Parisian, HealthSouth, Compass Bank and Humana. She also serves as a member of the Alabama and Birmingham Bar Associations.