EPSTEIN BECKER GREEN | HEALTH CARE & LIFE SCIENCES CLIENT ALERT

Thought Leaders in Health Law®

Third Update: Enforcement Deadline Extended To November 1, 2009

Do the FTC Red Flag Rules Apply to You? What Every Health Care Entity Should Know About the New Requirements to Prevent Identity Theft

by H. Carol Saul and Alicia Hayes Sable

July 2009

Third Update: Enforcement Deadline Extended to November 1, 2009

Set forth below is our October 2008 Client Alert notifying hospitals and health care providers of the requirements to comply with the FTC Red Flag Rules, including the requirement to adopt a written identity theft prevention program. The original compliance deadline was November 1, 2008. Subsequent to our initial release of the Client Alert, the FTC extended the enforcement deadline. The first extension was until May 1, 2009, but on the eve of that deadline, the FTC announced that it would delay the enforcement until August 1, 2009. Just days before the anticipated August 1, 2009 enforcement deadline, the FTC announced that the date on which it will commence enforcement of the Red Flag Rules has been further extended to November 1, 2009.

It appears that the delayed enforcement is the result of pressure from several groups, including trade associations and governmental committees, who are concerned about the fact that there is a great deal of confusion as to which entities must comply with the Red Flag Rules. In a July 29th press release, the FTC stated that in order to "assist small businesses and other entities, the Federal Trade Commission staff will redouble its efforts to educate them about

compliance with the 'Red Flags' Rule and ease compliance by providing additional resources and guidance to clarify whether businesses are covered by the Rule and what they must do to comply. To give creditors and financial institutions more time to review this guidance and develop and implement written Identity Theft Prevention Programs, the FTC will further delay enforcement of the Rule until November 1, 2009." The FTC has posted guidance and resources on its website for entities that are trying to determine whether they are subject to the Red Flag Rules. This FTC website is available at: www.ftc.gov/redflagsrule

The FTC continues to emphasize that the rules themselves are not changing, but that the announcement merely suspends enforcement of these rules until November 1, 2009. This compliance extension again gives hospitals and affected providers some breathing room; however, it is still critical for each entity and provider to move forward with its analysis of whether it meets the definition of a *creditor* with *covered accounts* in order to determine whether it must adopt a written identity theft prevention program by November 1, 2009. We will continue to monitor any further developments in this area. Please refer to our Web site at www.ebglaw.com for further information and updates.

October 2008

Security breaches at hospitals and other health care entities are occurring with alarming frequency, as evidenced by the nearly daily news stories covering this critical issue. While the threat that a security breach could result in identity theft of an entity's customers is a concern facing all consumer-based industries, recent reports have focused on the fact that health care entities seem to be particularly vulnerable to security breaches. Health care entities are a ripe target for security breaches due to the sensitive nature of the patient information that they house, such as personal identifying information (address, date of birth, social security number, etc., of a patient) and financial information (patient's account numbers, credit card numbers, etc.). The unfortunate reality is that health care entities and providers must fend off not only the traditional form of identity theft, which is an unauthorized acquisition or use of data that compromises the security, confidentiality, or integrity of a patient's personal information, but also medical identity theft. Medical identity theft, which is on the rise due to the increasing numbers of uninsured individuals, occurs when someone falsely uses another person's name or insurance or benefits information in order to obtain medical services or products, such as prescription pharmaceuticals. Medical identity theft can be devastating to the individual whose information was fraudulently used. It also presents financial, operational, and administrative difficulties for health care providers.

Applicability of The Red Flag Rules to Hospitals and Other Health Care Entities

The Federal Trade Commission ("FTC") has promulgated final regulations in conjunction with The Fair Credit Reporting Act, as amended in 2003,[1] requiring financial institutions and other creditors, by **November 1, 2008**, to adopt written identity theft

prevention programs designed to prevent, detect, and mitigate the effects of identity theft. Such regulations, known as the "Red Flag Rules,"[2] are applicable to any entity that meets the definition of a *creditor* and maintains *covered accounts*, regardless of whether the health care provider is a for-profit or not-for-profit entity.

A *creditor* is defined as any entity that "*regularly* extends, renews, or continues credit; [or] any [entity] who *regularly* arranges for the extension, renewal, or continuation of credit."[3] During an American Health Lawyers Association teleconference on October 1, 2008, an attorney from the FTC (the "FTC Representative"), defined "credit" in very broad terms as the right granted to a debtor to defer payment for goods or services. There has been some speculation about whether there is a quantifiable definition of "regularly" extending or arranging for credit, which is relevant to an entity's determination as to whether it is a "creditor" who must comply with the Red Flag Rules. While the regulations do not provide a bright line test on this issue, the FTC Representative stated that, in her view, "regularly" is interpreted to mean a regularly occurring business practice. Accordingly, under her interpretation, hospitals and other health care providers are creditors if they, as a regular business practice, do not require all patients to pay for medical goods or services at the time that such goods or services are provided.

A *covered account* is an account used primarily for personal, family or household purposes, which involves multiple payments or transactions.[4] For example, offering extended payment plans to patients makes an entity a "creditor" that offers "covered accounts." In order to determine whether an entity maintains "covered accounts," the entity must conduct a risk assessment, which takes into account the methods it uses to open accounts, the access to such accounts, and the entity's previous experience with identity theft.[5] This risk assessment must be conducted as an initial matter, and also must be conducted on a periodic basis in order to determine the applicability of the Red Flag Rules to that entity.

Written Identity Theft Prevention Program

Hospitals and other health care providers that are "creditors" and maintain "covered accounts" must comply with the Red Flag Rules by implementing a ***written*** identity theft prevention program. This written identity theft prevention program must be approved and adopted by the Board of Directors or equivalent governing body.[6] This written identity theft program must contain policies that:

- **Identify** "red flags", including relevant patterns, practices and/or activities that potentially implicate identity theft (see examples below);

- **Detect** the "red flags" that are identified in the program;

- **Respond** to "red flag" incidents that are detected in order to prevent and mitigate the effects of identity theft; and

- **Ensure** that the program is reviewed and updated periodically in order to adjust to

changing and developing identity theft risks.

The patterns, practices, incidents or activities that constitute "red flags" of identity theft will vary based upon the particular entity's operations. However, entities may find that the "red flags" will fall under some or all of the following categories: 1) alerts, notifications or warnings received from a consumer credit reporting agency, 2) the presentation by individuals of suspicious documentation that appears to be altered or inconsistent with other documents on file, 3) the submission of suspicious personal identifying information, such as multiple addresses, 4) unusual or suspicious use of or access to a patient's covered account, or 5) notification from patients or law enforcement authorities indicating suspected or actual identity theft.

While each written identity theft prevention program must contain the four fundamental elements listed above, the manner in which such written policies are implemented should be based upon the size and scope of the entity, itself. In other words, one size does not fit all. Each entity should tailor its program to be appropriate for its operations, its patients, and its technological capabilities. Importantly, hospitals and other health care entities should identify and incorporate into their program "red flags" of medical identity theft in addition to traditional financial identity theft. Implementation of an appropriate program will likely require coordination between information technology personnel, management personnel, and then ratification by the Board of Directors.

Compliance Deadline and Implementation

The deadline to comply with the Red Flag Rules is November 1, 2008. This deadline is rapidly approaching, especially for entities in the health care field that may have been unaware of these rules. However, as the FTC Representative emphasized, these requirements should not cause panic within the health care community. First of all, it is likely that a health care entity's HIPAA Privacy and Security Policies already include several of the protective and preventative measures that are required under the Red Flag Rules. Second, although the FTC has the authority to impose a penalty of $2,500 per incident of a knowing violation of the regulations, the FTC Representative stated in the same teleconference that, from an enforcement perspective, the entity need only show that it is making "reasonable, good faith" efforts to comply with the rules by November 1 if such entity's Board of Directors cannot approve and adopt a full written identity theft prevention program by that date.

Other Laws Relating to Security Breaches and Identity Theft

In addition to the Red Flag Rules, security breaches and potential customer or patient identity theft implicate other laws and regulations. Approximately 45 states have enacted security breach notification laws,[7] which require entities that experience a security breach that compromises identifying personal information, to report such breaches to certain authorities and to notify the affected individuals, often within a very short timeframe. If you experience a security breach, please refer to your state security breach law or contact counsel in order to take the steps necessary to comply with these notification requirements in a timely manner.

* * *

For questions regarding this alert and topic, please contact:

H. Carol Saul
Atlanta
404/923-9069
Csaul@ebglaw.com

Alicia Hayes Sable
New York
212/351-4514
Asable@ebglaw.com

The EpsteinBeckerGreen Client Alert is published by EBG's Health Care and Life Sciences practice to inform health care organizations of all types about significant new legal developments.

Lynn Shapiro Snyder, Esq.
EDITOR

If you would like to be added to our mailing list or need to update your contact information, please contact, Jennifer Sunshine, jsunshine@ebglaw.com or 202/861-1872.

Endnotes

1 15 U.S.C. § 1681 *et. seq*.
2 16 C.F.R. § 681
3 15 U.S.C. § 1681a(r)(5), 1691a 16 C.F.R. § 681.2(b)(4) (emphasis added).
4 16 C.F.R. § 681.2(b)(3).
5 16 C.F.R. § 681.2(c).
6 16 C.F.R. § 681.2(e).
7 As of October 1, 2008, the following states have enacted security breach notification laws: Alabama, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Louisiana, Maine, Maryland, Massachusetts, Michigan,

Minnesota, Nebraska, Nevada, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin and Wyoming.