JUDICIAL DIAGNOSIS

The FTC Red Flags Rule
Requirements of Healthcare Providers For Compliance

Linn Foster Freedman, JD

On February 26, 2009, the Federal Trade Commission (FTC) reported identity theft as number one, for the ninth year in a row, on its list of top consumer complaints received in 2008. The FTC received over 1.2 million consumer complaints in 2008; the 313,982 identity theft complaints accounted for 26% of the total. The FTC has proposed identity theft regulations known as the Red Flags Rule that require mandatory compliance by healthcare providers no later than August 1, 2009. Although the **American Medical Association (AMA)** and other related entities have challenged whether or not healthcare entities are required to comply with the Red Flags Rule, in a February 4, 2009, correspondence to the AMA, the FTC declared that health care providers are subject to the Red Flags Rule.

The Red Flags Rule require physicians and hospitals to develop and implement written identity theft prevention programs to identify, detect and mitigate against theft when "red flags" are present by August 1, 2009. The purpose of the Rule is to try to prevent identity theft.

Health care providers must be concerned about medical identity theft, which is the misuse of another individual's personal information (such as a name, date of birth, social security number or insurance policy number) to obtain or bill for medical services or goods because the result can harm patient care, if a provider utilizes incorrect information to treat a patient. In addition, health care providers may be unable to bill and receive payment for services performed on a patient who is perpetrating a fraud.

To comply with the FTC Red Flags Rule, healthcare providers must develop and implement a written program with policies and procedures in place by August 1, 2009, to detect, prevent and mitigate identity theft, including policies to identify red flags and incorporate red flags into its compliance program, detect red flags that have been incorporated into the program, respond to any red flags that are detected to prevent and mitigate identity theft and ensure that the program is updated periodically. The Board of Directors or managers of the entity must approve the Red Flags Rule program. The program should be overseen, implemented and administered by a member of the Board or senior level management, should be updated and reviewed at least annually and employees should be trained with respect to what red flags are applicable to the entity and how to respond to those flags. In addition, any Business Associate Agreements must be amended to include that all business associates of the healthcare provider also comply with the Red Flags Rule.

What does this mean for small or large practices? It means that a written program must be developed and employees supervised on proper practices for authenticating every patient through obtaining corresponding forms of identification and responding to suspicious documents, inquiries or complaints. The Red Flags Rule Program developed for the practice should be tailored to the size and experience of the practice, and should not be burdensome to implement.

The Red Flags Rule went into effect for health care providers in Rhode Island on August 1, 2009. A non-complying entity may be subject to civil action by the FTC. In the case of knowing violations, fines of up to $2500 for each violation can be assessed.

Linn F. Freedman, JD, is a partner, Nixon Peabody LLP.

Disclosure of Financial Interests

The author has no financial interests to disclose.

CORRESPONDENCE

Linn Foster Freedman, JD
Nixon Peabody LLP
One Citizens Plaza, Suite 500
Providence, RI 02903
Phone: (401) 454-1108
e-mail:lfreedman@nixonpeabody.com