



## Identity theft compliance for physicians

By William H. Maruca, Esq.

Published December 2008

Identity theft is an unwelcome and often devastating byproduct of our modern digital age. Most media attention has been focused on financial wrongdoing involving credit card numbers, credit history and fraudulently obtained loans, as well as the trafficking in false identification associated with terrorist activity. The consequences of theft and misuse of health care records can be just as severe. In fact, the increasing economic and government pressure on health care providers to adopt electronic billing and medical records systems over the past decade has made the health sector a target-rich environment for criminals.

Under rules adopted pursuant to the Fair and Accurate Credit Transactions Act of 2003 by the Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration (NCUA), certain financial institutions and creditors will be required to implement a program to detect, prevent and mitigate instances of identity theft. These regulations, referred to as the "Red Flag" rules, require financial institutions and creditors to develop and implement written identity theft prevention programs. These programs must provide for the identification, detection and response to patterns, practices or specific activities – known as "Red Flags" – that could indicate identity theft.

But physicians aren't banks, lenders or credit card companies, so why is this their problem? Doesn't HIPAA provide enough privacy protection for patients? Many experts thought so, until some FTC attorneys said otherwise.

### Who is a "Creditor"?

The FTC says a creditor is any entity that regularly extends, renews or continues credit; any entity that regularly arranges for the extension, renewal or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew or continue credit. However, merely accepting credit cards as a form of payment does not in and of itself make an entity a creditor. The entity must extend

credit to, or accept deferred or installment payments from its clients, customers or patients.

Earlier this year, some FTC staff attorneys took the position that physicians are "creditors," and therefore subject to the Red Flag rules, if they do not require full payment at the time they see patients, and suggested that physicians who accept insurance are considered "creditors" if the patient is ultimately responsible for medical fees, including co-pays, deductibles or non-covered services. The American Medical Association wrote to the FTC on September 30, 2008 objecting to these interpretations and cited court cases in which similar activities were held not to be the extension of credit. The FTC has indicated that a response to the AMA's letter will be forthcoming.

Compliance was originally required by November 1, 2008, but the enforcement deadline has now been extended to May 1, 2009. During the six-month extension, the AMA continues to push the FTC to clarify whether and how these rules will apply to physicians.

A physician practice that qualifies as a creditor and that offers or maintains covered accounts must develop and implement a written Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft. A program must, at a minimum, be adopted by the owners, board of directors or other governing body; be designed to identify and detect and respond appropriately to Red Flags; be updated periodically to reflect changes in risks from identity theft; designate responsibility for the program at the senior management level; and provide staff training and effective oversight.

Like HIPAA compliance, Red Flag compliance is "scalable" with regard to the size of the organization. A one-doctor practice will not be held to the same standards as a 10-hospital health system.

### **What are Red Flags?**

The FTC identifies the following categories of Red Flag events in its guidance, applicable to all affected creditor entities, not just health care providers:

- Alerts, notifications or other warnings received from consumer reporting agencies or service providers, such as fraud detection services.
- The presentation of suspicious documents.
- The presentation of suspicious personal identifying information, such as a suspicious address change.

- The unusual use of, or other suspicious activity related to, a covered account.

- Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

The World Privacy Forum published a list of Red Flag indicators which may arise in the health care industry and warrant identification and investigation:

- 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; or an Explanation of Benefits or other notice for health services never received.

- Records showing medical treatment that is inconsistent with a physical examination or medical history as reported by the patient, i.e. substantial discrepancies in age, race, and other physical descriptions.

- A complaint or question from a patient about the receipt of a collection notice from a bill collector.

- A patient or insurance company report that coverage for legitimate hospital stays are being denied because insurance benefits have been depleted, or that a lifetime cap has been reached.

- A complaint or question from a patient about information added to a credit report by a health care provider or insurer.

- 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 notice or inquiry from an insurance fraud investigator for a private insurance company or a law enforcement agency.

Once suspicious activity has been identified and flagged, a covered health care provider will need to have a plan for evaluating whether identity theft has occurred, and how to mitigate its effects. The FTC guidance states that appropriate responses may include:

- Monitoring a covered account for evidence of identity theft.
- Contacting the customer.
- Changing any passwords, security codes or other security devices that permit access to a covered account.
- Reopening a covered account with a new account number.
- Not opening a new covered account.
- Closing an existing covered account.
- Not attempting to collect on a covered account or not selling a covered account to a debt collector.
- Notifying law enforcement.
- Determining that no response is warranted under the particular circumstances.

### **More Than Money at Risk**

When an identity thief obtains health care services under a stolen identity, records of those services can become commingled with the victim's legitimate health records. Not only do insurers and other third party payors get stuck with fraudulent bills, but the victim's health may be jeopardized by inaccurate medical history, prescriptions, procedures, chronic conditions, etc. Once such fraudulent information is identified, it is recommended that the victim's chart be flagged and all extraneous data be extracted from the victim's record and maintained separately, either under a "John/Jane Doe" file, or if the identity thief is identified, under the thief's name.

### **What to Do During the 6-Month Reprieve?**

Although it may be tempting to Google "Medical Identity Theft Policy," download the first one you see and put your name on it, that approach is likely to create more problems than it solves. Like canned HIPAA and Medicare compliance programs, a canned Red Flag policy may be broader than you need and may include features that are impractical or impossible for your practice to follow. In the event of a dispute, you will be held to the terms of the policy you adopt, so be careful about what your policy includes. You should work with experienced health care counsel to develop a program that fits your own practice's needs, meets the FTC's requirements as

they are clarified, and is practical and feasible for you and your staff to implement.

*William H. Maruca, Esq., is a partner with the Pittsburgh office of Fox Rothschild LLP who concentrates his practice in the area of health care.*

## [Obtain Medical Specialty Own-Occupation Disability Insurance On-line](#)

© 1996-2007, Physician's News Digest, Inc. All rights reserved.

### **Local Medical News**

<a href="#">Philadelphia Metro Edition</a>	<a href="#">Eastern PA Edition</a>	<a href="#">Western PA Edition</a>	<a href="#">New Jersey Edition</a>
<a href="#">Cover Story</a>	<a href="#">Cover Story</a>	<a href="#">Cover Story</a>	<a href="#">Cover Story</a>
<a href="#">Spotlight Interview</a>	<a href="#">Spotlight Interview</a>	<a href="#">Spotlight Interview</a>	<a href="#">Spotlight Interview</a>
<a href="#">News Briefs</a>	<a href="#">News Briefs</a>	<a href="#">News Briefs</a>	<a href="#">News Briefs</a>
<a href="#">Editor's Notebook</a>	<a href="#">Editor's Notebook</a>	<a href="#">Editor's Notebook</a>	<a href="#">Medicine &amp; Computers</a>
<a href="#">Commentary</a>	<a href="#">Commentary</a>	<a href="#">Commentary</a>	<a href="#">Medicine &amp; the Law</a>
<a href="#">Medicine &amp; Computers</a>	<a href="#">Medicine &amp; Computers</a>	<a href="#">Medicine &amp; Computers</a>	<a href="#">Medicine &amp; Business</a>
<a href="#">Medicine &amp; the Law</a>	<a href="#">Medicine &amp; the Law</a>	<a href="#">Medicine &amp; the Law</a>	<a href="#">Personal Finance</a>
<a href="#">Medicine &amp; Business</a>	<a href="#">Medicine &amp; Business</a>	<a href="#">Medicine &amp; Business</a>	
<a href="#">Personal Finance</a>	<a href="#">Personal Finance</a>	<a href="#">Personal Finance</a>	

Physician's News Digest | 117 Forrest Ave | Narberth | PA | 19072 | 800-220-6109  
[info@physiciansnews.com](mailto:info@physiciansnews.com)