Identity Theft Programs: What Every Anesthesia practice Should Consider Doing Now

Neda Mirafzali
The Health Law Partners, P.C.

NEWSFLASH: As of July 29, 2009, the Federal Trade Commission ("FTC") extended its August 1 deadline to enact the commonly referred Red Flags Rule (16 C.F.R. Part 681) to November 1.

Come November 1, anesthesia practices, among other entities, will be responsible for ensuring patients' identity protection under the provisions of the Red Flag Rule. Constituting 5% of all identity theft, medical identity theft has gained greater political attention and media coverage; thus, the Red Flags Rule should come at no surprise. According to the FTC, medical identity theft occurs when an individual seeks medical services using another's name and insurance information. It is not until victims check their credit history or are denied insurance coverage for a medical service for having reached their policy limit that they realize their identity has been stolen and their credit history crushed, taking years to revitalize. Additionally, erroneous medical entries are recorded in the victim's name producing a fictitious medical history. The recent extension is to give the FTC additional time to "redouble its efforts to educate [entities] about compliance with the 'Red Flags' Rule and to ease compliance by providing additional resources and guidance to clarify whether businesses are covered by the Rule and what they must do to comply." The FTC announced that, in the future, it would make available additional resources

and compliance guidance for low-risk entities.

What is the Red Flags Rule?

In short, the Red Flags Rule requires particular entities to develop and implement *reasonable* policies and procedures—appropriate to the size and complexity of the entity—to guard against identity theft. As part of the Fair and Accurate Credit Transactions Act of 2003 ("FACT"), financial institutions and creditors must have anti-identity theft programs in place. According to the FTC, "red flags" are any factors that could indicate identity theft, including identification, detection, and response to patterns, practices, or specific activities. Under the Red Flags Rule, the FTC requires financial institutions and creditors to do the following:

- *Identify* relevant patterns, practices, and specific forms of activity that are "red flags" signaling possible identity theft and incorporate those red flags into the Identity Theft Prevention Program;
- *Detect* red flags that have been incorporated into the Identity Theft Prevention Program
- *Respond* appropriately to any red flags that are detected to prevent and mitigate identity theft; and
- *Ensure* the Identity Theft Prevention Program ("Program") is updated periodically to reflect changes in risks from identity theft.

Who Has to Comply with the Red Flags Rule?

The FTC declared that the Red Flags Rule requires each financial institution and creditor that holds any covered account, "to develop and implement an Identity Theft Prevention Program…for combating identity theft in connection with new and existing accounts."

For physician practices, the relevant definition is that of a creditor. A creditor, as defined in the regulation, is a "person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit."

A covered account, as defined in the regulations, is an account "that involves or is designed to permit multiple payments or transactions…and any other account…for which there is a reasonably foreseeable risk to members or to the

safety and soundness of the federal credit union from identity theft…."

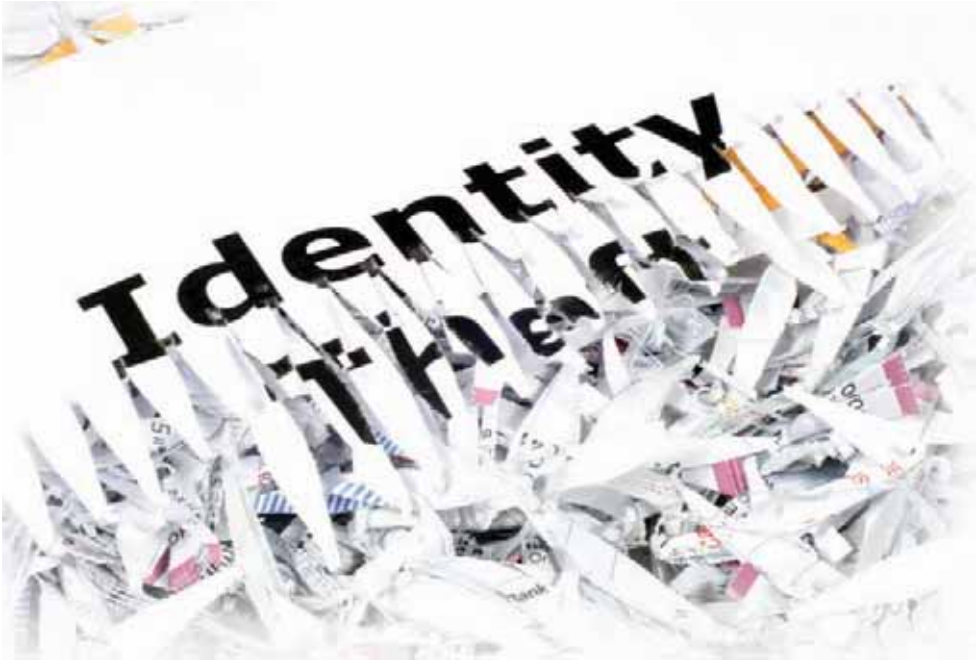
How Does the Red Flags Rule Apply to Physician practices?

Though many physicians question the reasons why this applies to their practices, the FTC insists that *the Red Flags Rule applies to physician practices*. Physician practices that accept insurance or allow payment plans are considered creditors as they allow deferred payment until physicians render the services and collect the insurance and other applicable payment owed. As a result, physician practices are subject to the Red Flags Rule.

Even with this definition, however, many physician practices do not agree that they are creditors under the definition of creditor. Thus, the FTC provides examples of why it believes a physician practice is a creditor. For example, a physician practice is a creditor if it "regularly bill[s] patients after the completion of services, including for the remainder of medical fees not reimbursed by insurance." This language would cover most, if not all, anesthesia practices. Additionally, if a physician practice allows patients to set up a payment plan, the physician practice would be considered a creditor and would, therefore, be subject to the Red Flags Rule.

Not all physician practices are required to adopt the Red Flags Rule. Those physician practices that require full payment prior to rendering services are not creditors and are not subject to the Red Flags Rule. Merely accepting credit card payments does not render a physician practice a creditor.

The American Medical Association (AMA) does not agree with the FTC's position asserting that such position is not "consistent with the intent or scope of the enabling legislation…." To



date, the AMA's protests have not been successful. This is further highlighted by the FTC's new publication entitled, "The 'Red Flags' Rule: What Health Care Providers Need to Know About Complying with New Requirements for Fighting Identity Theft" (http://www.ftc.gov/bcp/edu/pubs/articles/art11.shtm).

How Can Anesthesia practices Comply with the New Regulations?

Generally, anesthesia practices ("practices") rely on their respective hospital or facility to gather information on admitted patients. It is important that anesthesia practices check that the hospital or facility has an Identity Theft Program in place that complies with the requirements of the Red Flags Rule and any other applicable state law. practices should coordinate with the facility to adopt applicable portions of the facility program into the practice's program to assist in meeting its Red Flags Rule obligations.

Administrative Responsibilities

The regulations require certain administrative action and oversight. For example, prior to implementing a program, the practice must have its Board of approve the proposed program. Also, practices must designate a person to be involved in oversight of the program and education of staff. Furthermore, the regulations require that covered creditors take steps to oversee that their service providers, like billing and management companies, conduct business according to the procedures designed to mitigate the risk of identity theft. Accordingly, practices should contact their billing companies and request a copy of their policies/procedures on this topic.

As stated above, there are four parts to complying with the Red Flags rules: identifying red flags, detecting red flags, responding to red flags, and ensuring an updated program. Notably, all protocols adopted in compliance with the Red Flags Rule must be in writing.

Identify and Detect

There is no complete enumeration of approved ways to identify medical identity theft. However, the FTC has

Continued on page 12

IDENTITY THEFT PROGRAMS: WHAT EVERY ANESTHESIA PRACTICE SHOULD CONSIDER DOING NOW

Continued from page 11

provided examples of warning signs to look for. Practices should be aware of suspicious documents, suspicious personally identifying information, suspicious activities, and notices from victims, law enforcement, or insurers of possible identity theft. The FTC suggests physician practices ask the following questions:

- Has the new patient given you identification documents that look altered or forged?
- Is the photograph or physical description on the ID inconsistent with what the patient looks like?
- Did the patient give you other documentation inconsistent with what he or she has told you?
- Did the patient give you information that is inconsistent with what is on file?
- Is mail returned repeatedly as undeliverable while the patient still shows up to appointments?
- Does a patient complain about receiving a bill for a service that he or she did not get?
- Is there an inconsistency between a physical examination or medical history reported by the patient and the treatment records?

If one answers "yes" to any of these questions, it would be beneficial to ask for additional information from that patient to ensure the individual's identity matches the claimed identity. Again, since the practice will likely rely on facility personnel to obtain documentation in the admission process, the practice should ensure that the facility requests and verifies patient identification and resolves any discrepancies as they arise prior to rendering the actual service. In such cases, the practice's written program should refer to the facility's written procedures for this verification process and should attach such written procedures.

Respond

After a red flag has been identified and detected, the practice should follow a procedure to respond to the red flags. Responding to red flags could include a plan for gathering documents if there is an incident, a process for reporting the incident to the appropriate personnel, and guidelines to follow for appropriate action (i.e. stopping the admission and billing process, notifying the person whose identity was used, notifying the authorities, assessing the impact on the practice, etc.). In the case of an anesthesia practice, for those flags detected in the facility admission process, the practice would be relying on the facility to take action and coordinate with the practice. Again, the practice's written program would need to record that the facility's procedures for identifying and responding to issues have been adopted by the practice. For those issues identified after the service has been rendered, but during the billing process, the practice would need to make sure that the billing process has been halted and that appropriate action is taken. This must be included in the practice's written program.

Ensure

While this program is in place, it is important for practices to continuously update the practice's procedures to ensure that they are consistent with most recent updates and developments surrounding medical identity theft.

State law

In addition to addressing the FTC regulations, practices should also check state law for any requirements related to this topic. For example, some states have enacted laws protecting social security numbers. State law requirements can easily be incorporated into the practice's written Identity Theft Program. The local or State medical society is a good place to begin researching state law.

Summary

Though there are no criminal ramifications for failing to comply with the Red Flags Rule, there are financial penalties for non-compliance, including a $2500 fine for each *known* violation. For those practices who need assistance in developing their written program, a qualified healthcare law firm can help. For additional guidance, please visit the FTC website at www.ftc.gov and the FTC's guidance to healthcare providers, http://www.ftc.gov/bcp/edu/pubs/articles/art11.shtm.

Neda Mirafzali is a third year law student at Michigan University College of Law. She wrote her article while working as a law clerk at The Health Law Partners, P.C. The firm represents hospitals, physicians, and other health care providers and suppliers with respect to their health care legal needs.