Published on Auntminnie.com
May 26, 2009

READYING FOR THE RED FLAGS RULE

BY: MARK F. WEISS, J.D.

In order to give "creditors," which by definition includes many radiology groups and imaging facilities, more time to comply with its "Red Flags Rule," the Federal Trade Commission has announced that it will delay enforcement of the Rule until August 1st.

What is the Red Flags Rule?

The Red Flags Rule is federal regulation aimed at detecting identity theft through the identification by financial institutions and creditors of "red flags," indicators of possible identity theft appropriate to the specific business relationship, in order that action can be taken to expose actual instances of that crime, mitigate its damage, and prevent future occurrences.

Despite protest by the American Medical Association and other groups that the federal statue pursuant to which the Red Flags Rule was issued was never meant to cover the patient-provider relationship, and that, therefore, the Rule is overbroad, the FTC has not agreed with that position.

In announcing the extension of the enforcement date, the FTC acknowledged the debate concerning the scope of the Rules and stated that it will release a template to help entities that have a low risk of identity theft, including those that know their customers personally, comply with the law.

Why Should Radiologists and Imaging Facilities be Concerned?

Radiologists and imaging facilities need to be concerned with the Rule and compliance with it for several reasons.

First, the penalty for noncompliance with the Rule could be as high as $2,500 for each "knowing violation." As it is likely that an entity's noncompliance would be global and not just limited to a single instance, it is conceivable that an entity liable for one penalty would be simultaneously liable for many penalties.

Second, there are other good reasons to comply with the Rule besides the avoidance of penalties:

- The Rule operates as a logical component to patient privacy laws including HIPAA, with which your practice already complies. HIPAA and other privacy laws are designed to keep a patient's healthcare information restricted to those who should be using it – the Red Flags Rule operates to prevent a patient's healthcare information from being "polluted" with inapplicable data, the data of a third party who has assumed the patient's identity. In this light, the Red Flags Rule is another component of assuring data security and trustworthiness.

- Unpolluted data not only benefits the "real" patient, in certain circumstances it can benefit your ability to interpret and diagnose. For example, it increases the chances that an image taken previously is really of the same individual.

- Additionally, it increases the odds that you will not be conned into providing care that will not be reimbursed. For example, Ms. Jones' carrier will not pay for services delivered to Ms. Smith masquerading as Ms. Jones.

How Can I Determine if my Practice is Required to Comply With the Rule?

The Rule sets out a test to determine if you fall within its scope.

First, you must be a "creditor" which, for medical practices or facilities, means that you regularly defer payment by your patients through accepting payment from their carrier or by allowing payment plans.

If you are a creditor, the Rule applies only if you have "accounts," which requires a continuing relationship with your patients. Although it might be conceivable that your practice has one-time patient encounters only, most if not all practices will have multiple transactions with some patients and will therefore fall subject to the Rule.

The next step is to determine if your accounts are "covered accounts." There are two tracks to covered account status. One is that the service underlying a multiple payment account relates to personal, as opposed to business, purposes; most healthcare services would be included within this track. The other track is that there is a reasonably foreseeable risk of harm (financial, operational, compliance, reputation, or litigation risk) to your "customers" or to your practice from identity theft.

We're Covered, So Now What?

If your practice or facility is covered by the Rule, you are required to implement a written "Identity Theft Prevention Program" by August 1, 2009. The Program must be approved by your entity's board of directors or like governing body or by senior management.

The first step in developing the Program is to identity "red flags" of identity theft relevant to your operation. For example, red flags might include identification that is obviously forged or phony, a social security number outside of the date range of the patient's stated age, an address which turns out to be nonexistent or otherwise not valid, or receipt of a complaint from the person receiving your statement that he or she has never been a patient of your practice.

You have to design and implement procedures for identifying those red flags, both in respect of new patient accounts and existing ones. This includes staff training on the implementation of policies designed to discover incidents of red flags.

You need a plan for how to react if a red flag is detected. Your plan might include steps such as informing the police and other authorities, notifying the victim of the identity theft, and assessing the injury to your practice and its medical records.

Your Identity Theft Prevention Program must be overseen by your entity's board, senior management or by someone to whom that task is delegated. And, you need to make periodic assessments of how your plan is operating and of any changes to it that should be made.

What's the Practical Bottom Line?

From a practical perspective, it makes little or no sense to rely on the argument that the Red Flags Rule or the statute underlying it is overbroad and not meant to apply to healthcare providers.

Even if the FTC were to change its position on the applicability of the Rule, it is beneficial to radiologists and imaging facilities to adopt its practices to reduce the risk that you might be creating medical data that "pollutes" your medical records, and that increases the chances that you will be paid for your services.

Lastly, compliance is relatively easy, especially when considered as a complement to existing HIPAA policies and procedures.

___

Mark F. Weiss is an attorney who specializes in the business and legal issues affecting anesthesia and other physician groups. He holds an appointment as clinical assistant professor of anesthesiology at USC's Keck School of Medicine and practices with The Mark F. Weiss Law Firm, a firm with offices in Los Angeles, Santa Barbara and Dallas. He can be reached by email at markweiss@weisspc.com and by phone at 310-843-2800.