Are You Red Flag Ready?

Cheyenne Brinson, MBA, CPA; for KarenZupko & Associates, Inc.

Enforcement of the Federal Trade Commission's (FTC's) Red Flags Rule ("the Rule") has been extended again—this time to June 1, 2010. This is the fourth time the Rule has been delayed since it was initially set to roll out on November 1, 2008.

The Rule mandates that creditors institute policies and procedures to prevent identity theft.[1] Since physicians don't typically think of themselves as creditors, the American Medical Association (AMA) and other specialty societies did not believe that the Rule applied to physician practices and wrote a letter to the FTC asking them to exempt physician practices.[2] Despite their attempts, the FTC maintained that the Rule does apply to physician practices.[3] Why? Because the FTC contends that not demanding payment up front and later billing insurance is a form of extending credit. Bottom line—as it stands now, the Rule applies to physician practices. And maybe that's not a bad thing.

Why Is This Important?

Besides being mandated by the FTC, there are practical reasons why the provisions of the Rule are important to your practice.

For starters, medical identity theft is the fastest growing form of identity theft in America today—accounting for 3% of identity theft crimes, or 249,000 of the estimated 8.3 million people who had their identities stolen in 2005, according to the FTC.[4] The number of medical identity theft crimes is predicted to be much higher today.

Take the story of Maria, an illegal immigrant who stole an incarcerated woman's identity for Medicaid benefits to receive $530,000 worth of treatment for cervical cancer.[5] Or John who stole the identity of a mentally disabled friend to pay for his heart bypass surgery.[6]

Medical identities—that is, valid insurance cards—are being stolen and sold on the street for about $50 per identity whereas a stolen Social Security number (SSN) has an estimated street value of $1 per identity.[7]

Is it possible that a medical identity thief could come to your practice? This will not only cause the victim financial harm, but what do you do when you now have the medical histories of two people intertwined?

Ms. Brinson is Consultant and Speaker, KarenZupko & Associates, Inc., Chicago, Illinois.

Address correspondence to: Cheyenne Brinson, MBA, CPA, KarenZupko & Associates, Inc., 625 N Michigan Ave, Suite 2225, Chicago, IL 60611 (tel, 312-642-5616 ext 220; fax, 312-642-5571; e-mail, cbrinson@karenzupko.com; Web site, www.karenzupko.com).

***Am J Orthop.* 2009;38(12):630-632.**

Protect Your Practice Today

The heart of the Rule is to *verify that all patients are who they say they are*. The easiest way to do that is to check a form of photo identification (ID), eg, driver's license. Best practice is to scan the photo ID into the practice management system or take a picture of the patient. This creates a baseline to compare with the next time the patient comes in. It's also good documentation that you are following the Rule.

What Else Does the Rule Say?

The Rule mandates that a *written* identity theft prevention program is in place whose purpose is to:

1. Identify relevant Red Flags based on the risk factors of the medical practice.
2. Institute policies and procedures to detect Red Flags.
3. Identify steps the practice will take to prevent and mitigate identity theft.
4. Identify appropriate responses to Red Flags, should they occur.
5. Create a system of administrative oversight and periodic updating of the program.

Identify Red Flags

There are four common Red Flags for most physician practices; these are the things that your staff must be alert to and looking out for:

1. *Suspicious documents*. First and foremost, does the person standing in front of you look like the picture on the photo ID? Does the ID appear to be forged or altered?
2. *Suspicious personal identifying information*. Examples of this would be that a patient provided the same SSN as another patient, or the patient has the same name and date of birth as another patient.
3. *Suspicious activity*. Are there any inconsistencies with the medical record and the information the patient is giving during the consultation?
4. *Actual notice of identity theft*. An obvious Red Flag is to receive notice from a patient, a victim of identity theft, or from law enforcement that identity theft has occurred. Another common Red Flag is to receive a complaint or inquiry from an individual who received a bill for services, even though they have never been to your practice.

Detect Red Flags

Unless you personally know the patient, require all new patients to submit a valid photo ID issued by a local,

Frequently Asked Questions

Question: Can we keep a copy of our patients' ID, such as their driver's license, on file in our practice management system?
Answer: Yes. As long as you are compliant with the Health Insurance Portability and Accountability Act (HIPAA), you may scan the ID obtained into your practice management system. In fact, we recommend this so that you have a baseline to compare identification with the next time the patient comes in. Plus, it's documentation that you verified the patient's identity. Some practices are opting to take a picture of the patient—that works too.

Question: What do we do with credit card information we have for patients on payment plans or for our cancellation policy?
Answer: You want to keep written authorizations for up to 18 months—in case a patient disputes the charges. However, you must keep these documents secure, preferably in a locked drawer and limiting access only to necessary staff.

Question: Our practice obtains Social Security numbers (SSNs). Can we still do this?
Answer: Absolutely! There are patients who are reluctant to give out their SSN. However, for anyone who has ever turned over a patient to collections, you understand the value of having their SSN. For insurance patients who refuse to give their SSN, you may want to consider collecting full payment up front. In essence, you are extending credit to patients—that is why you need their SSN.

Question: What do I do when patients don't have an ID or get upset that they must show an ID?
Answer: Explain to them that you are doing this to help them—you want to be sure that someone else isn't using their identity. As for patients without a driver's license, you can ask for other forms of ID, such as a state-issued ID card or a voter's registration card. The KZA sample policy includes a list of acceptable IDs (sample policy available at: http://www.karenzupko.com/resources/forms.html).

Question: We keep credit card information in our practice management system including the credit card number and expiration date. For the Red Flags Rule, can we still keep this information?
Answer: As long as your practice management system is Payment Card Industry (PCI)–compliant, then all is well. Any system that houses card-holder data must be vetted by the card associations to verify compliance with PCI. If your practice management system has completed their PCI compliance, they should have a certificate of validation from Visa. For more information on PCI compliance, contact your credit card processing solution or Brian Bickel at Solveras Payment Solutions at brian@Solveras.com.

state, or federal government agency (eg, driver's license, passport, or military ID) and include in each patient's file a scanned copy of the ID as submitted. In the case where the new patient is a minor, obtain a photo ID of the patient's parent or guardian, and, in the case where a new patient does not have a valid photo ID, obtain two forms of non-photo ID, one of which is issued by a state or federal agency (eg, birth certificate, Social Security card, voter registration card, lawful permanent residence card, or "Green Card").

For patients paying by credit card, confirm that the name on the credit card matches the patient's photo ID. The same applies to patients paying by personal check—ensure that the name on the personal check is the same as that on the ID.

Prevent and Mitigate Identity Theft

In the event that identity theft is suspected, immediately stop the billing process: Do not bill an insurance company, accept a personal check or credit card, or set a patient up for a payment plan until the patient can satisfactorily provide information to verify identity.

Investigate any allegations or complaints of identity theft and make a determination of whether the billing or payment was made fraudulently.

Appropriate Responses to Red Flags

In the event that a Red Flag is identified, take the following actions as appropriate:

1. Notify the individual whose identity was compromised.
2. Cease collection efforts on the account.
3. Notify law enforcement.
4. Notify private insurance carrier, Medicare, or Medicaid.
5. In the event of actual fraud, offer the affected individual free credit-monitoring service for one year.
6. Flag the affected patient's chart for an alert that a Red Flag exists for this patient.
7. Determine that no response is warranted under the particular circumstances (ie, suspicious-looking identification turns out to be a false alarm).

Administrative Oversight and Periodic Updating of the Program

Another element of an identity theft prevention program is to designate the person or persons who are responsible for administration of the program. This might be your Board of Directors, a committee of the Board, Managing Physician, or another employee at a senior management level, such as

Practice Administrator. A medical assistant, a biller, or a front desk staff person, for example, is not the appropriate person to administer the plan.

A sample identity theft prevention program is available for free at http://www.karenzupko.com/resources/forms.html.

Author's Disclosure Statement and Acknowledgments

The author reports no actual or potential conflict of interest in relation to this article.

Watch an encore presentation of the free Red Flags Rule webinar featuring KZA associate Cheyenne Brinson, MBA, CPA, sponsored by Solveras Payment Solutions. It includes implementation checklists and policy samples you can customize for your practice—saving you time and money! The webinar can be watched at http://learningcenter.karenzupko.com/programs.html.

References

1. Identity theft red flags and address discrepancies under the Fair and Accurate Credit Transactions Act of 2003. *Fed Regist.* 2007;72(217):63718-63775. To be codified at 16 CFR Part 681.
2. American Academy of Dermatology Association, American Academy of Facial Plastic and Reconstructive Surgery, American Academy of Family Physicians, et al. Coalition letter asking for clarification of the FTC Red Flags rules application. September 24, 2008. Medical Group Management Association (MGMA) Web site. http://www.mgma.com/policy/default.aspx?id=22230. Accessed October 5, 2009.
3. Harrington E. Letter from the FTC re: Red Flags rule. February 4, 2009. Medical Group Management Association (MGMA) Web site. http://www.mgma.com/WorkArea/showcontent.aspx?id=26876. Accessed October 5, 2009.
4. Federal Trade Commission. FTC releases survey of identity theft in the U.S. Study shows 8.3 million victims in 2005. Federal Trade Commission Web site. http://www.ftc.gov/opa/2007/11/idtheft.shtm. Published November 27, 2007. Accessed October 5, 2009.
5. Olivo A. "I only wanted the pain to end." *Chicago Tribune.* March 15, 2009. http://archives.chicagotribune.com/2009/mar/15/local/chi-medical-id-theftmar15. Accessed October 5, 2009.
6. St Clair S, Hood J. Man stole pal's identity to pay for bypass surgery, police say. *Chicago Tribune*. August 22, 2008. http://archives.chicagotribune.com/2008/aug/22/health/chi-heart-scam_22aug22. Accessed October 5, 2009.
7. McKay J. Identity theft steals millions from government health programs. *Government Technology*. February 13, 2008. http://www.govtech.com/gt/260202?topic=117677. Accessed October 5, 2009.