Red Flags Rule and Identity Theft Prevention: You Don’t Have To, But You Should!

June 1, 2010 Update: Red Flags Rule is delayed for the 5th time, now until December 31, 2010. Read my post here. Also see resources under the Library tab.

Mandatory adherence to the Red Flags Rule is delayed. Again.

So? So, why do medical practices have to be forced to do the right thing? Confirming patient identities is the right thing for so many reasons. Yes, it is one more thing in the long line of things that practices have had to fold into the mix of administrative tasks associated with, but not really related to, the care of patients. But it is the right thing to do.

Taking the role of the patient (because I am one), this is why I want my personal physician to adhere to the Red Flags Rule:

- I once had my driver’s license stolen and the thief or buyer of my information opened a cell phone account and ran up a $600 bill before I realized my driver’s license was gone. I got off easy, relatively speaking, but it took hours and hours on the phone to get everything straightened out. It was also frightening. I do not care to experience this again.
- If someone used my medical insurance to get care paid for, I wonder how I might find out. Maybe when my application for life insurance was turned down for illnesses or conditions I never had? Maybe when someone had run up a bill in my name and creditors came knocking? Maybe never, yet I could suffer the consequences without knowing the reasons why.

- I would wonder why my physician wasn't implementing policies to protect me against identity theft. Is he too busy? Too lazy? Too complacent? What else is he lagging behind on?

So, why haven't you implemented a program in your practice?

Will Your Medical Practice Be Ready on May 1, 2009 for the Red Flags Rule?

I am very pleased to have had the opportunity to interview **Ester Horowitz, the founder and CEO of M2Power, Inc.,** and the voice of sanity among the current confusion surrounding the Red Flags Rules.

The **Federal Trade Commission (FTC) states that the Red Flags Rule:**

> *was developed pursuant to the Fair and Accurate Credit Transactions Act (FACTA) of 2003. Under the Rule, financial institutions and creditors with covered accounts must have identity theft prevention programs to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft. The Rule applies to creditors and financial institutions.*

Most medical practices have been identified as creditors under the Red Flags Rule. The FTC defines a health provider as a creditor if they "bill consumers after their services are

completed. Health care providers that accept insurance are considered creditors if the consumer ultimately is responsible for the medical fees." Note that being a creditor is not linked to whether you take credit cards or not.

Creditors then must determine if they have "covered accounts." The FTC states that "A covered account is used mostly for personal, family, or household purposes that involves multiple payments or transactions. This includes continuing relationships with consumers for the provision of medical services."

Horowitz has written an excellent article on the Red Flags Rule and is receiving calls weekly from medical practices asking her for guidance. She notes that many practices are having trouble distinguishing between the new Red Flags Rule and the existing HIPAA standards, and practices may think that compliance with HIPAA meets the criteria for the Red Flags Rule. Horowitz says emphatically, "There is a distinct difference between PHI (Protected Health Information) and what the Red Flags Rule considers "identity" information." Although there may be some overlap in HIPAA and the Red Flags Rule, existing HIPAA programs will not be sufficient to keep a practice from incurring fines, if identity theft is traced to the medical practice.

Horowitz outlines the fines as follows:

> *Employee or Customer information lost under the wrong set of circumstances may cost a company or practice:*
>
> *Federal and State Fines of $2500 per occurrence*
> *Civil Liability of $1000 per occurrence*
> *Class action Lawsuits with no statutory limitation*
> *Responsible for actual losses of Individual ($92,893 Avg.)*

Note the word "employee" in the paragraph above. The medical practice is responsible for the information contained in

“employee applications, payroll data, W-2, social security numbers, drivers licenses, and credit cards, military records, and birth certificates” as well as information derived from consumers.

What are the requirements of the Red Flags Rule? A creditor with covered accounts must:

1. Develop a written program, approved by its board of directors, that identifies warning signs and suspicious activity of possible identity theft.
2. Develop measures to prevent identity theft must be implemented.
3. Mitigate damages from instances of identity theft.
4. Ensure that staff is be trained/retrained periodically.

How does one detect identity theft? It is rarely easy, therefore one typically only finds out after the fact. For medical practices, asking for picture ID each and every time the patient is seen might be the only way to determine identity. It would make excellent sense for insurance cards to have photos on them, however, we are all changing insurance policies so often now that this does not seem feasible. Some practices routinely copy the new patient’s driver’s license. Others take photos of the patient and store them in the paper record or digitally in the EMR.

Horowitz points out that fake IDs are quite common, as your teenagers could probably tell you. With the number of people losing insurance coverage when they lose their jobs, can we expect in new black market in fake insurance cards?

The other problem that Horowitz describes is that of mixing care for two different people, one the actual person and the second the identity thief. She notes that practices have a “medical responsibility to find and treat the right person.”

I asked Horowitz about the issue of using the social security number as a patient identifier in medical practices. Many

practices require the pateint's social security number, as it still is the single most useful number for matching patient identities and for collection purposes. She said "Use of the social security number in healthcare is not going away any time soon. Remember that Medicare cards still use the social as its basis. Practices must do everything in their power to limit the exposure to that number and to protect it."

Horowitz also noted that every system devised will have its thieves – something like "build it and they will break it." She feels that the critical piece is to have monitoring systems in place to be alerted to the first signs of identity theft so that the ramifications can be minimized. She suggests that practices educate their employees as to the devastating (financial and emotional) effects of identity theft, and encourage personal monitoring programs. Whether a practice decides to provide these programs as an employee benefit is a decision each will have to make. Providing coverage for employees would certainly be a strong indicator of proactive intent to protect the employee if an employee's identity was stolen from information housed with the employer. Horowitz also recommends that practice provide patients with literature about identity theft (not required by the Red Flags Rule), and especially let the patients know if any process in the practice will be changing (e.g. showing a photo ID at every visit.)

As for the new compliance programs for Red Flags, Horowitz can provide a customized program, employee education, and a monitoring model so the practice is ready for the May 1, 2009 deadline for having the program in place. The deadline is less than 55 days away – do you have your program in place?

More about Ester Horowitz:

Ester Horowitz is founder of M2 Power Inc, and serves as practice marketing and business advisor for the medical industry working with doctors, chiropractors, LCSWs and other

health professionals. She helps implement marketing & business actions plans within the professional codes of ethics, HIPAA, and fraud and abuse compliance obligations. Her nationally acclaimed publications focus on the business of medicine and include such articles as "The Death of Dr. CEO", "How to Find $50,000 in Your Practice", "What Does Buying, Selling, and Growing a Practice Have in Common", "When Selling a Practice What is Important to Know", a video "" "Raising Capital", and her book The Blatant Truth of Owning a Medical Practice: Rx for Practice Owners.