

What You Don't Know Can Hurt You: Meeting Red Flag Regulations

While Protecting Against Medical Identity Theft

By Nancy Vickroy

With the enforcement of Red Flags Identity Theft Prevention Program compliance which went into effect May 1, 2009, many healthcare organizations have already employed measures to comply with these rules while also protecting themselves against dangers of medical identity theft. These measures differ somewhat from other industries because they must also comply with the Red Flag regulations such as financial institutions, primarily due to the nature of medical care.

To better understand the special nuances of Red Flags in the healthcare industry, the following information highlights various aspects of the regulations as well as analysis conducted by TransUnion.

Already an Issue

One of the primary reasons Red Flags play a special role in healthcare is because medical identity theft already has cost the industry millions of dollars. In fact, the Federal Trade Commission conducted a recent survey estimating that three percent of identity theft victims had their personal information used to obtain medical services by another person — impacting approximately 250,000 U.S. patients in 2005. This translates to an estimated \$468 million in medical identity crimes per year.

As the economy has worsened, the potential for increased identification theft has increased. In fact, data breaches increased 47 percent in 2008, according to the Identity Theft Resource Center. And 13 of 100 recent data breaches as of March 2009 (1.3 million files) reported were direct theft from healthcare providers or insurers, potentially impacting over 98,000 patients — doubling the 2005 identity theft from healthcare from 3 percent to 7 percent of all identity thefts.

Medical identity theft, in turn, exacerbates the growing bad debt issue that hospitals face, since the usual reason for medical identification theft is to use someone else's medical insurance for care. Therefore, it makes good business sense for healthcare providers to take steps to protect against identity fraud as well as good medical safety sense since serious medical errors can result from mixed identities on medical records, such as wrong blood types or allergies.

Types of Red Flag Alerts and Study Results

Most of the identity validation processes underlying the new Red Flag regulations probably aren't new to most hospitals, but these processes may not have been documented on a front and back-end process continuum. What may be new to many providers is the Red Flag regulatory suggestion to validate patient's identity documentation with external databases, particularly from credit reporting agencies to determine if that identity information has a fraud alert or other warning. Many healthcare providers are using revenue cycle solutions that now offer specific Red Flag alerts, like TransUnion's Revenue Manager as an integral part of their patient identity verification software.

The regulations list 26 examples of Red Flags. The examples range from alerts received from an external data source to having a training staff be vigilant on common identity fraud schemes. To learn which alerts may be most common, TransUnion sampled 800,000 of its healthcare customers' 2009 first quarter inquiries. The study results highlight several types of Red Flags alert categories: warnings from a consumer reporting agency, suspicious personal identifying information, and consumer fraud notices. Overall, 7.4 percent of patients in the study had at least one alert. Often, multiple alerts were triggered if suspicious information was supplied.



Risk Assessment Areas in Healthcare

When developing an identity theft prevention program, a hospital should go through a risk assessment of areas or procedures where opportunities may exist for fraudulent activity. The two most likely areas are:

- Up front, in-patient intake such as pre-registration or registration functions, where false documentation or stolen identification forms may be presented. Unlike many financial services that are also required to comply with Red Flags, healthcare is typically a face-to-face encounter, which makes checking identity documentation easier.
- At the back end, in-patient account and billing functions where irregular patterns of non-payment, undelivered mail, or fraud notices occur when trying to collect for a patient account.

The depth of a hospital's risk assessment will vary, usually according to the complexity of its organization. A provider in a small community will probably not need the same protocols as an urgent care center in a large city. The assessment should map out how identity data flows throughout the organization — who collects it, who reviews it, who stores it and who retrieves it.

Staff Training

When designing the identity theft prevention programs and the related Red Flags, it's imperative that healthcare administrators make sure the alerts are easy to understand and actionable by their staff. In addition, since many healthcare encounters are face-to-face, the hospital staff should be carefully trained to know what they should — and should not — do if they suspect fraud.

A Red Flag alert could be due to something as minor as a typographical error or missing a street type when compared to an external validation source. Or it could be a more egregious warning that indicates a possible

medical identity fraud, such as a stolen Social Security number. Hospitals need to train for caution, discretion and clarity in order to protect them from a potentially dangerous position of accusing someone of l'd theft. Instead, staff should be trained to mark account for exception handling after the patient has received emergent treatment.

Conclusion

While there is no panacea for healthcare providers — or any organization for that matter — to ensure effective identity management, knowing what to look for as well as mapping out data flows and robust staff training can help hospitals understand some of the unique challenges within healthcare versus other organizations that must also comply with the Red Flag Regulations.

Nancy Vickroy is the director of product development in TransUnion's healthcare group. She can be reached at nvickro@transunion.com.

Content Management Got Your Head Spinning?



Integrated Solutions — Where ECM Technologies Come Together

Integrated Solutions is a publication designed for IT decision makers interested in learning how the latest ECM technologies can improve business operations. In each issue, you will learn how companies successfully integrate complementary ECM technologies throughout their enterprises. You'll also learn about the cost justification for these projects and the subsequent benefits.

Some of the core technologies you'll find in every issue of *Integrated Solutions* include:

- Content Management
- Forms Processing
- Document Imaging
- Workflow



For a FREE subscription, go to ISMinfo.com

Integrated Solutions
FOR ENTERPRISE CONTENT MANAGEMENT

Integrated Solutions • Knowledge Park, 5340 Fryling Road, Suite 300, Erie, PA 16510 • Phone: (814) 897-9000 • ISMinfo.com