TransUnion®

TRANSUNION WHITE PAPER

Red Flag Regulations: Exploring the Impact of New Identity Theft Prevention Regulations on Healthcare Providers

Medical identity theft is a serious issue. The FTC conducted a recent survey estimating that 3 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.[1] Therefore, it makes good business sense for healthcare providers to take steps to protect against identity fraud.

Now healthcare providers may have an additional incentive to ensure that appropriate measures are in place to protect against the impact of identity theft. In July 2006, the national financial institution regulatory agencies and the Federal Trade Commission proposed new guidelines pursuant to the Fair and Accurate Credit Transaction Act of 2003 ("FACTA"). These guidelines are generally referred to as the Red Flag Regulations. The final Red Flag Regulations were released on October 16, 2007.

The two most relevant components of the Red Flag Regulations for healthcare providers are the requirements that:

1. Users of credit reports develop reasonable procedures to respond to notices of address discrepancies that they may receive from a credit reporting agency (See 16 CFR 681.1)

2. Financial institutions and "creditors" develop and maintain a comprehensive identity theft prevention program (See 16 CFR 681.2)

While the effective date for the regulations was November 1, 2008, the FTC delayed enforcement of the requirements with respect to 16 CFR 681.2 until June 1, 2010 to give financial institutions and "creditors" more time to develop their identity theft programs. This delayed enforcement does not apply to the other agencies that may have an enforcement role with respect to the Red Flag Regulations nor to the enforcement by the FTC of 16 CFR 681.1 which began on November 1, 2008.

TransUnion offers a full suite of fraud and identity management solutions that can help healthcare providers address certain regulatory obligations, including:

Establishing written policies and procedures for preventing, detecting and responding to identity theft.

Developing and applying reasonable policies and procedures to verify change of address requests and notifications.

Maintaining and updating policies and procedures to respond to evolving identity theft trends within the organization.[2]

Note: The Federal Register "Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003: Final Rule" was used as a general guideline in the writing of this document, located at: http://edocket.access.gpo.gov/2007/07-5453.htm

What is the impact of the Red Flag Regulations on healthcare providers?

The Red Flag Regulations include 26 illustrative examples of Red Flags associated with potential identity theft (see Appendix A). For purposes of the regulation, Red Flags are a pattern, practice or specific activity that indicates the possible risk of identity theft.

A healthcare provider may be subject to the requirements of two sections of the Red Flag Regulations, sections 16 CFR 681.1 and 16 CFR 681.2.

1. Section 16 CFR 681.1 applies to any "user" of credit reports

A healthcare provider may use credit reports from TransUnion or another source for a "permissible purpose" such as making a decision about whether to extend credit or provide insurance to an individual or for employment purposes. Doing so makes the healthcare provider a "user" of credit reports for purposes of the Red Flag Regulations.

What may be required for healthcare providers: Address Discrepancies

Section 16 CFR 681.1 of the Red Flag Regulations requires a healthcare provider that is a user of credit reports to maintain reasonable procedures to respond when it receives a notice of an "address discrepancy" from the credit reporting agency that is providing a credit report. The procedures should be designed to allow the healthcare provider to "form a reasonable belief that a credit report relates to the consumer about whom it was requested." In other words, this section requires that the healthcare provider take reasonable steps to confirm that the individual with whom it is dealing is truly who he or she claims to be.

The Regulations give some examples of how this may be accomplished, including comparing the address shown on the credit report against information it maintains in its own records, against data it acquires from a third party or directly from the consumer. In summary, a healthcare provider needs to take reasonable steps to review the address on a credit report against information it receives from another source.

Although it is not currently common for healthcare providers to furnish credit data to credit reporting agencies for inclusion in credit reporting databases, it is still worth noting that there is an additional requirement for users of credit reports who do routinely furnish data. Such furnishers of data are required to report reasonably confirmed addresses to the credit reporting agency that initially provided the notice of an address mismatch.

2. Section 16 CFR 681.2 applies to all financial institutions and creditors

A healthcare provider is most likely not a financial institution for purposes of the Red Flag Regulations but may be considered a "creditor." For purposes of the regulations, the agencies use the definition of "creditor" from the Equal Credit Opportunity Act ("ECOA") which says that a creditor is "any person who extends, renews or continues credit; any person that regularly arranges for the extension, renewal or continuation of credit; or an assignee of an original creditor who participates in the decision to extend, renew or continue credit." "Credit" under the ECOA means a "right granted to defer payment for any purchase." Therefore, any healthcare provider or other entity that provides a product or service for which the recipient pays later is a "creditor."

What may be required for healthcare providers: identity theft prevention program

The requirements of Section 16 CFR 681.2 are a bit more complex. Under this section, a healthcare provider that is a creditor must implement an identity theft prevention program. This program must be designed to detect and prevent identity theft in connection with the opening or maintenance of a "covered account."

What is a covered account?

A "covered account" is defined very broadly; the term covers traditional situations where delayed or multiple payments are allowed by a creditor with regards to personal or household purchases (i.e., credit card accounts, mortgage loans, utility accounts), but it also covers any other account with a creditor where there is a reasonably foreseeable risk of identity theft that would harm the consumer and/or creditor. For those healthcare providers that meet the definition of "creditor" for the purposes of these regulations, it is likely that they maintain the type of covered accounts for which the requirements are directed.

Developing an identity theft prevention program in the healthcare setting

In developing its identity theft prevention program, a healthcare provider should note four key steps which will be instrumental in preparing to meet compliance with the Red Flag Regulations.

Step 1: Identify appropriate Red Flags

The first step is to determine which Red Flags will be used in detecting potential identity theft at a healthcare provider's facility. While the regulators provided a list of possible Red Flags (see Appendix A), a healthcare provider is free to choose those Red Flags that make sense in its environment.

To identify which Red Flags to incorporate into its procedures, a healthcare provider will want to identify all departments within its organization that may interact with an individual with a covered account. Once these departments are known, the healthcare provider will want to determine what types of information are gathered, and how that information is verified.

Step 2: Detect Red Flags

Next, healthcare providers should develop procedures to detect Red Flags during the life of the account. In the healthcare setting, there may be opportunities to spot Red Flags at various stages of a covered account including:

Pre-registration

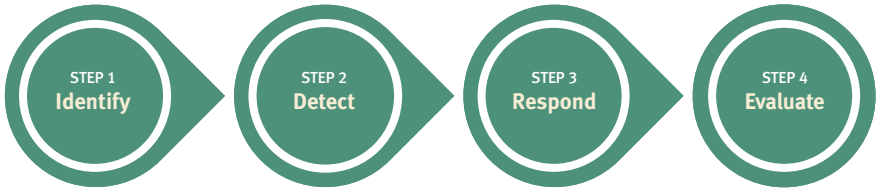
Registration

Financial Counseling

Billing and Collections

Therefore, a common approach to identity verification should be implemented at every step. A breakdown in any one area increases the potential risk of identity theft.

Four steps to implement an identity theft prevention program



Source: TransUnion

Potential Red Flags for healthcare providers

Patient Registration (Customer Acquisition)	Alerts from Credit Reporting Agency
	Suspicious documentation
	Suspicious personally identifiable or household information
Patient Billing Accounts (Customer Management)	Unusual or suspicious activity
	Notice from consumers or others

For example, verifying identity could include asking for a photo id such as a driver's license or passport and checking that information against the patient's established account or insurance card. Verifying identity should also examine if the document is possibly forged by determining if the photo id matches that of the patient or if the date of birth corresponds to the patient's apparent age.

Some healthcare providers are incorporating automated solutions into their identity management processes with tools that allow providers to verify and authenticate identity information such as name, address, date of birth, phone number and Social Security number (if applicable). Authenticating identity information could include checking the provided identity information against an external set of databases such as from a Consumer Reporting Agency, known fraud databases, or the Social Security Administration.

CASE STUDY:

Detecting fraud at one Midwest hospital

TransUnion looked at high-risk fraud alert files for one of its healthcare customers located in a suburb of one large Midwestern city. In the first nine months of 2008, 391 fraud alert matches were discovered at the hospital. The transgressions ranged from a "Social Security number not being issued by the Social Security Administration" to an "address reported being used in true name fraud or credit fraud" situation.

Authentication should also check the integrity of the provided data to answer questions such as:

Does the name match the address?

Is the address a residential address or perhaps a business warehouse?

Does the phone number match the address?

If applicable, is the Social Security number issued by the Social Security Administration or was it used in a death benefit claim?

Step 3: Respond to Red Flags

Healthcare providers must develop a plan to respond to any Red Flags that are detected. As healthcare providers prepare responses to any potential Red Flags, it's important to remember that responses will vary depending upon which Red Flag is triggered and the magnitude of the risk associated with it. It's also important to train staff members in the appropriate policies, procedures and responses to ensure a consistent experience for patients while also balancing the provider's commitment to the community.

For example, if a healthcare provider receives an alert that the patient's provided name and address does not match against external validation sources, the staff member should flag the account for follow-up and use objective coaching scripts to help guide what could be a sensitive, potentially difficult conversation with the patient.

Step 4: Evaluate the program

Make sure that the identity theft prevention program is periodically evaluated for effectiveness and modified as needed to address changes in the risks posed by identity theft to consumers and creditors. As the program matures, those responsible for its administration should track any known incidents of identity theft that occurred despite the program as well as any shifts in trends associated with identity theft in the marketplace. This data will enable the administrators of the program to make meaningful modifications to the program over time.

Beyond these four elements of an identity theft prevention program, the Regulations also include certain administrative requirements.

Executive management oversight and approval

In order to be in compliance with the Red Flag Regulations, a healthcare provider will need to ensure that the identity theft prevention program it develops is approved by its executive management or board of directors and that the appropriate oversight is in place by these organizational leaders. This demonstrates the healthcare provider's commitment to identity theft prevention and ensures that a measure of accountability is built into the program.

Staff training

Just as the success of an identity theft prevention program will be dependent upon the involvement of those at the highest level of the organization, so too does it depend upon the understanding and participation of those throughout the organization who may have a role in preventing identity theft.

Therefore the Red Flag Regulations also require a program to include a process to provide training for relevant staff members. All staff members that open and access covered accounts must be trained regarding the policies and procedures that are applicable to their job function. This would include training upon hiring, refresher training as needed, and training on new policies or procedures when the Red Flag program is updated.

Third-party vendors

Finally, in addition to the roles of executives and staff members, the Red Flag Regulations acknowledge that healthcare providers may use third-party service providers that can also play a role in identity theft prevention. As part of its program, a healthcare provider should review its relationships with service providers and where necessary, make sure that such service providers are contractually bound to take measures similar to those required of the healthcare provider to detect and prevent identity theft.

Helping to ensure more effective identity management

There is no panacea for healthcare providers—or any organization for that matter—to ensure effective identity management. Medical identity theft can victimize patients multiple times in multiple provider settings, sometimes across several states. As a result, patients have to work closely with their providers to monitor their healthcare files.

The goal of an effective identity management program is to provide a reasonable level of assurance and trust for both healthcare providers and patients. Patients passing verification are presented for authentication. Healthcare providers can achieve the strongest confidence level in identity management when a patient successfully passes both verification and authentication.

In addition to meeting the obligations of the Red Flag Regulations, this approach should meet these high-level business requirements:

Mitigate fraud losses

Reduce operational costs

Improve patient safety

Effective mitigation will require the use of new technologies and approaches within a healthcare provider's existing fraud prevention policy. Identity management must be integrated within the revenue cycle process as well as the medical record process. Strong patient authentication will support numerous technologies and account management best practices.

By validating and authenticating accurate patient identities at the beginning of a new patient-provider relationship, healthcare providers are better able to manage security throughout the relationship. Additionally, a comprehensive identity theft prevention program can mitigate losses for healthcare providers and improve their relationship with patients.

APPENDIX A

Examples of Red Flags

These examples of Red Flags have been summarized from "Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003," pages 89-90.

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1	A fraud or active duty alert is included with consumer report.
2	A consumer reporting agency provides notice of a credit freeze in response to a request for a consumer report.
3	A consumer reporting agency provides a notice of address discrepancy.
4	A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity for an applicant or consumer, such as: **a.** Recent and significant increase in the volume of inquiries. **b.** An unusual number of recently established credit relationships. **c.** A material change in the use of credit, especially with respect to recently established credit relationships. **d.** An account was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5	Documents provided for identification appear to have been altered.
6	The photograph or physical description on the identification is not consistent with the appearance of the applicant or consumer presenting identification.
7	Other information on the identification is not consistent with information provided by the person opening a new account or consumer presenting the identification.
8	Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.
9	An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10	Personal information provided is inconsistent when compared against external information sources used by the financial institution or creditor. **For example:** **a.** The address does not match any address in the consumer report; or **b.** The Social Security number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
11	Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
12	Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by financial institutions or creditors. **For example:** **a.** The address on an application is the same as the address provided on a fraudulent application; or **b.** The phone number on an application is the same as the number provided on a fraudulent application.
13	Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. **For example:** **a.** The address on an application is fictitious, a mail drop, or prison; or **b.** The phone number is invalid, or is associated with a pager or answering service.

APPENDIX A (continued)

Suspicious Personal Identifying Information (Continued)

14	The SSN provided is the same as that submitted by other persons opening an account or other customers.
15	The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
16	The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
17	Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.
18	For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19	Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for new, additional or replacement cards or cell phone, or for the addition of authorized users on the account.
20	A new revolving credit account is used in a manner commonly associated with known patterns of fraud. **For example:** **a.** The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or, **b.** The customer fails to make the first payment or makes an initial payment but no subsequent payments.
21	A covered account is used in a manner that is not consistent with established patterns of activity on the account. **There is, for example:** a. Nonpayment when there is no history of late or missed payments. b. A material increase in the use of available credit. c. A material change in purchasing or spending patterns. d. A material change in electronic fund transfer patterns in connection with a deposit account. e. A material change in telephone call patterns in connection with a cellular phone account.
22	A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
23	Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
24	The financial institution or creditor is notified that the customer is not receiving paper account statements.
25	The financial institution or creditor is notified of unauthorized charges in connection with a customer's covered account.

Notice from Consumers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institution or Creditors

26	The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

[1] Rys, Richard. "*An Imposter in the ER: Medical Identity Theft can Leave You with Hazardous Errors in Medical Records.*" Self. March 13, 2008.

[2] Office of the Comptroller of the Currency, Treasury (OCC); Board of Governors of the Federal Reserve System (Board); Federal Deposit Insurance Corporation (FDIC); Office of Thrift Supervision, Treasury (OTS); National Credit Union Administration (NCUA); and Federal Trade Commission (FTC or Commission). Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003. http://www.ftc.gov/os/2007/10/r611019redflagsfrn.pdf

The information contained in this White Paper is not intended as and in no way constitutes legal guidance and/or advice of any nature from TransUnion, nor is anything contained herein a guarantee that your fraud and identity management program will be compliant with Red Flag Regulations. TransUnion makes no warranties of any kind concerning the information provided in this White Paper. You must consult your own legal counsel or compliance advisor to determine whether your fraud and identity management programs will enable your organization to meet your compliance obligations associated with Red Flag Regulations.

TransUnion®