



**Effectively Addressing the New “Red Flag” Requirements
and Other Federal Healthcare Regulations**
nTelagent’s Self-Pay Management System as a Compliance Tool

An nTelagent, Inc. White Paper

www.ntelagent.com

nTelagent, Inc., 330 Mallory Station Road, Suite B-3, Franklin, TN 37067
615-866-0483
Updated 2009

Introduction

In today’s healthcare environment, it seems there are always new rules to live by. **And now, more than ever before, the actions of hospitals and other healthcare service providers are under increasing scrutiny, from multiple sources. Complying with the new “Red Flag” requirements, which become mandatory in 2009, is of particular concern.**

From protecting patient privacy, to mitigating medical identity theft, to ensuring appropriate debt collection methods are in practice, to accurately documenting charity care—providers all across the United States are struggling to not only keep abreast of changing regulations, but also to ensure that they consistently meet the requirements and can easily prove that they indeed have followed the rules at an auditable level.

This white paper focuses on how nTelagent’s Self-Pay Management System (SPMS) addresses the myriad of regulations concerning the handling of patient financial accounts, including the Red Flag Rules.

Similar to applications used in the retail industry at the point of sale, nTelagent’s SPMS tells healthcare registrars and financial counselors exactly what to do and what to say to each patient at the point of service regarding financial responsibilities. Using non-credit scoring data, SPMS provides interactive scripts that integrate patient demographic information with each provider’s business policies and rules. The system allows for price transparency and automatically identifies discounting, social services eligibility and charity care options when applicable, ensuring that patient financial accounting—for both insured and uninsured patients—is handled appropriately and consistently.

The system documents how every patient is treated from a financial perspective, tracking how each user (e.g., registrar, financial counselor) is handling each patient encounter, including charity eligibility and address discrepancy. From a provider’s perspective, these steps are critical in complying with the multitude of regulations relating to patient privacy, financial documentation and medical identity theft.

Overview of the “Red Flag and Address Discrepancy Rules”

“Healthcare organizations store a lot of valuable personal, identifiable information such as SSNs, names, addresses, age, in addition to banking and credit card information. This makes healthcare organizations extremely valuable targets because with this information scammers can develop complete profiles on victims making them ripe for identity theft.”

—SecureWorks Threat Analysis, 2/13/08

One of the most recent sets of regulations issued—called the “Red Flag and Address Discrepancy Rules”—comes from the Federal Trade Commission (FTC), in conjunction with other agencies. (A “red flag” is any pattern, practice or activity that could indicate identity theft.) These new consumer protection rules encompass a wide range of financial institutions and creditors, and require that such organizations address identity theft risks and develop and implement a mitigation plan. (See Appendix A for background on the rules.)

The regulations, which became effective January 1, 2008, now are causing quite a stir among healthcare service providers, and for good reason. First, many healthcare providers, whether for-profit, non-profit or government, may indeed have obligations under this new set of rules. A huge concern, medical identity theft is dealt with specifically in the Red Flag Rules. Second, there’s the issue of timing: Compliance with the Red Flag Rules becomes mandatory in 2009.

According to the World Privacy Forum’s report:
“Essentially, if a healthcare provider extends credit to a consumer by establishing an account that permits multiple payments, the provider is a creditor offering a covered account and is subject to the Red Flag Rules.” Those organizations that fall under the Red Flag Rules must develop and implement a written Identity Theft Prevention Program. The program’s purpose is to detect, prevent and mitigate identity theft in connection with new or existing covered accounts. (See Appendix B for details of the program’s required elements.)

What exactly is medical identity theft?

The World Privacy Forum (www.worldprivacyforum.org) defines medical identity theft as the following:

“Medical identity theft occurs when someone uses a person’s name and sometimes other parts of their identity – such as insurance information or Social Security Number – without the victim’s knowledge or consent to obtain medical services or goods, or when someone uses the person’s identity to obtain money by falsifying claims for medical services and falsifying medical records to support those claims.”

Because health records often contain patients’ home addresses, financial information (including credit card numbers), Social Security numbers and other information, they are a virtual treasure trove for identity thieves.

The FTC has not issued any specific “red flags” for healthcare service providers, but the World Privacy Forum has compiled a listing of suggested red flags in healthcare that would trigger an investigation. Some of these include the following: “a dispute of a bill by a patient who claims to be the victim of identity theft; patients having gotten a bill for another individual or a bill for a product or service they deny receiving; records showing medical treatment that is inconsistent with a physical exam or medical history reported by the patient; a patient or insurance company report that coverage for legitimate hospital stays is denied because insurance benefits have been depleted or a lifetime cap has been reached.” (Source: Fierce Healthcare, 9/29/08)

nTelagent’s SPMS as a Red Flag Compliance Tool

“As collections move from the back end to the front end, patient and credit privacy concerns are at the forefront. Providers must determine what type of information is most appropriate, and least vulnerable to attack. Our Self-Pay Management System works to manage and protect the necessary data, which in turn protects both the provider and the patient.”

—Earl T. Winter, nTelagent Chairman and CEO

The new Red Flag Rules can be overwhelming for hospitals and other healthcare service providers. Many are struggling to adopt systems and procedures that ensure and document compliance at every step of the process. **nTelagent’s Self-Pay Management System is a unique, easy-to-use and easy-to-implement web-based technology that is already helping healthcare organizations across the country with their compliance efforts.**

Looking specifically at the Red Flag and Address Discrepancy Rules, **SPMS helps hospitals and other providers to lessen the risk of identity theft from the outset with the Red Flag**

More information on the Red Flag and Address Discrepancy Rules is available on the FTC’s website at www.ftc.gov/opa/2007/10/redflag.shtm and www.ftc.gov/bcp/edu/pubs/articles/art11.shtm.

See also nTelagent’s issue brief on “Protecting Patient and Credit Privacy As Self-Pay Collections Move From the Back End to the Front End,” released April 2008, at www.ntelagent.com.

Compliance Report. In addition, the system enables users to identify many of the previously mentioned red flags—allowing them to determine when medical identity theft may be occurring and respond appropriately. With the Red Flag Compliance Report, nTelagent’s system allows real-time compliance reporting for an immediate ability to identify misuse of the system or fraudulent information. **Compliance can be monitored at a system-user/employee level and at a patient level.**

Let’s look at how SPMS works. Since the advent of health insurance options, including private insurance, Medicare and Medicaid, the focus of collections for healthcare service providers has been on the back end. But healthcare has shifted to a retail model. With more and more patients entering healthcare facilities and emergency rooms as self-pay patients, healthcare providers are facing the increasing challenge of collecting payments upfront, directly from the individual patients, who have assumed significant responsibility for paying for care.

In order to determine patient capacity to pay, some providers rely solely on obtaining a patient’s credit score, a risky proposition these days. In fact, those providers using credit reports and scores to determine patient capacity to pay or for other reasons also must follow yet another set

of rules and regulations under the Address Discrepancy section of the FTC’s rules. (See Appendix C for an overview of this section.)

Looking beyond the associated privacy risks, healthcare service providers who rely on credit data to determine capacity to pay should consider this type of information’s limitations. For example, a credit score does not necessarily give a good indication of whether a patient will pay a medical bill, as credit scores are based on voluntary purchases and medical debt is largely involuntary. Other limitations, such as security freezes and state and federal legislation, can also limit the usefulness and availability of a credit score. In addition, even a soft touch on a patient’s credit score can adversely affect his or her ability to get credit by lowering the credit score.

Instead of using an individual’s credit score, nTelagent’s system incorporates in-depth demographic information to help healthcare service providers arrive at a more accurate picture of patient financial responsibilities. **At the point of service, SPMS provides a risk-free approach to verifying patient information, using only a person’s name and address—no credit information is needed.** nTelagent’s solution helps to protect patients from the growing threat of identity theft because **the system does not use or store sensitive information such as credit scores, credit data, Social Security numbers or date of birth** (data elements that are extremely risky to hold and vulnerable to identity theft attacks—**from both outside and inside healthcare facilities**).

SPMS compares a patient’s biographical data with nTelagent’s proprietary database, giving healthcare service providers instant, actionable information and interactive scripting—telling healthcare registrars and financial counselors exactly what to do and what to say to each patient at the point of service about pricing of services, discounting, terms, and charity and government programs if appropriate. In addition, SPMS automatically generates forms at the point of service, giving patient access staff the capability to obtain signatures for payment arrangements, ensuring patients are aware of financial responsibilities from the start.

Verification of a patient’s identity, as well as his or her capacity to pay for services, is delivered to patient access staff in a matter of seconds, with no need for the paper-based proofs of identity of yesterday. The database returns the most recent recorded address for the guarantor, not a list of addresses that the individual has used in the past. The system alerts the registrar or financial counselor to any red flags regarding patient identity or fraudulent activity, and instructs them in how to handle the patient encounter. On the flip side, through its Red Flag Compliance Report, the system detects any suspicious activity or misuse of the data by an internal user (e.g., patient access staff and others) and alerts managers/administrators.

SPMS’s ability to immediately arrive at proof of patient identity is critical; without this function, providers open themselves up to fraudulent activity. If a healthcare facility can not absolutely prove that individuals are who they say they are, there can be major negative consequences: higher fraud rates, including people using multiple identities or insurance information that is not theirs; the potential delivery of incorrect medical treatment; and the possibility that charity care and government assistance programs are not being properly allocated. **The key is collecting adequate and accurate data at the front end, and then having it organized in a manner that allows for instantaneous, appropriate action and decision making.**

In sum, here’s how SPMS’s Red Flag Compliance Report can help providers with their Identity Theft Protection Program under the Red Flag Rules:

- **Mitigate the risk of medical identity theft**, including patients’ use of multiple identities or Social Security numbers that don’t belong to them and other illegal activities, by verifying and validating patient identity at the point of service
- **Avoid collecting and storing risky patient data that is vulnerable to attack (from inside or outside sources)**, such as credit score information
- Arrive at a **more accurate picture of patient financial responsibilities** at the point of service, allowing providers to efficiently categorize accounts
- **Lower the number of denied insurance claims** because every detail is verified and validated at the point of service
- Ensure that patients receive the **correct medical treatment / financial assistance**
- Keep the patient contact database **clear of inaccuracies**
- Meet charity care guidelines and audits due to **automated, consistent categorization**

How SPMS Addresses Other Regulations’ Requirements

Let’s turn away from the Red Flag Rules and explore some of the other regulations and guidelines healthcare service providers must follow. To illustrate just how SPMS helps hospitals and other providers ensure compliance, following are a few examples of regulations at the federal level:

Regulation / Guideline	How SPMS Addresses
<p>The Department of Health & Human Services Office of Inspector General (OIG) Advisory Opinion No. 08-03, issued in early 2008, outlines appropriateness of prompt-payment discounts for patients who pay their share of their medical bills quickly.</p>	<p>OIG requires that discounts be offered at the point of service. With SPMS implemented, service providers can offer discounts at the point of service, taking into account a patient’s current capacity to pay, total account balance and type of service. This enables the required fairness and consistency in the discounting process.</p>
<p>The Internal Revenue Service (IRS) 990 Schedule H requires that non-profit hospitals demonstrate their financial commitment to serving their community through charity care programs (mandatory in the 2009 tax year).</p>	<p>SPMS automatically screens patients at the point of service for charity care eligibility, with pre-built forms that determine and document care in a consistent and non-discriminatory manner.</p> <p>By classifying charity care at the point of service, SPMS helps providers to avoid sending these accounts to collections or writing them off as bad debt. (According to a recent nTelagent study of over 40 healthcare providers’ aged trial balance reports, of the accounts that were written off as bad debt, 17% were classified as having low household income and/or low net worth. This indicates that they could have been evaluated for government assistance programs or charity care processing, but were not.)</p>
<p>The Fair Debt Collection Law requires consistency in collection of hospital accounts.</p>	<p>SPMS allows healthcare providers to apply consistent collection, discounts and payment terms to every patient. In addition, the system ensures protection of patients’ rights by applying the proper recovery strategies to each person’s capacity to pay.</p>

Regulation / Guideline	How SPMS Addresses
<p>The Centers for Medicare and Medicaid Services (CMS) indicates indigent care should be supported by documentation.</p>	<p>SPMS provides online documentation of patients who potentially qualify as indigent or charity. The system also provides online application forms to be completed at the point of service. For healthcare providers looking to improve their handling and documentation of charity care cases, SPMS will:</p> <ul style="list-style-type: none"> • Eliminate inconsistencies in the choice of accounts to be reviewed for assistance • Provide consistency in application of charity care for those who do not qualify for assistance • Offer assistance to all patients meeting income guidelines • Allow healthcare providers to offer community benefits on a consistent basis by assisting patients in understanding their choices • Assist providers in meeting required application filing guidelines

nTelagent’s Self-Pay Management System additionally helps hospitals and other healthcare service providers to meet regulations and guidelines at the local and state levels. Because these vary significantly from location to location, we have focused on federal regulations here, which affect all areas.

Finally, as facilities prepare for CMS’s Recovery Audit Contractor (RAC) program, set to be expanded nationwide no later than January 1, 2010, the capabilities SPMS provides are even more important. nTelagent’s system can help facilities ensure a clean, effective revenue cycle management process and allow the facility to identify any inconsistencies within its compliance program. Reports from SPMS are auditable at the patient and system-user level.

The bottom line? SPMS automates and documents all patient financial encounters, ensuring compliance in a cost-effective, time-efficient manner. **By streamlining this aspect of their business, healthcare providers can focus on the most important things: delivering top-quality care, maintaining excellent patient relations and offering much-needed community benefits.**

About nTelagent, Inc.

nTelagent, Inc. has developed The Retail Application for the healthcare industry, called the Self-Pay Management System (SPMS). Similar to applications used in the retail industry at the point of sale, the company’s proprietary, automated system tells healthcare registrars and financial counselors exactly what to do and what to say to each patient at the point of service regarding financial responsibilities. Moving workflow to the front end of the revenue cycle, nTelagent helps providers ensure a better patient experience through clearer communication and better handling of patient accounts, while improving upfront and overall cash flow, receivables and profitability by reducing bad debt. Using non-credit scoring data, SPMS provides interactive scripts that integrate patient demographic information with each provider’s business policies and rules. The system allows for price transparency and automatically identifies discounting options, social services eligibility and charity care options when applicable, ensuring that patient financial accounting—for both insured and uninsured patients—is handled appropriately and consistently. Visit www.ntelagent.com for more information.

Appendix A The Fair Credit Reporting Act (FCRA) as amended in 2003 requires the Federal Trade Commission and bank regulatory agencies to issue joint regulations and guidelines regarding the detection, prevention, and mitigation of identity theft. The requirement includes special regulations directing debit and credit card issuers to validate notifications of changes of address under certain circumstances. 15 U.S.C. § 1681m(e). Another FCRA amendment calls for additional joint regulations offering guidance regarding reasonable policies and procedures that a user of a consumer report (e.g., a credit grantor) should employ when the user receives a Notice of Address Discrepancy. 15 U.S.C. § 1681c(h). These Red Flag and Address Discrepancy regulations were published in final form on November 9, 2007, 72 Fed. Reg. 63718 (Nov. 9, 2007). They are separate regulations. The mandatory compliance date for both rules is November 1, 2008. Although six agencies issued common regulations, the regulations that will affect health care providers are those from the Federal Trade Commission. 16 C.F.R. Part 681. The Federal Trade Commission will also be the agency that enforces the rules for the health care sector. *Source: Red Flag and Address Discrepancy Requirements: Suggestions for Health Care Providers, World Privacy Forum, 9/2008*

Appendix B For those creditors required to have an Identity Theft Prevention Program, there are four required elements. The program must include reasonable policies and procedures to:

1. Identify relevant Red Flags for the covered accounts that the creditor offers or maintains and incorporate those Red Flags into its program;
2. Detect Red Flags that have been incorporated into its program;
3. Respond appropriately to any Red Flags that are detected;
4. Update the program periodically to reflect changes in risks from identity theft to customers and to the safety and soundness of the creditor from identity theft.

There are also four elements to the administration of the Identity Theft Prevention Program. Each creditor required to have a program must:

1. Obtain approval of the initial written program from either its board of directors or an appropriate committee of the board of directors;
2. Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation, and administration of the program;
3. Train staff, as necessary, to effectively implement the program;
4. Exercise appropriate and effective oversight of service provider arrangements.

Source: Red Flag and Address Discrepancy Requirements: Suggestions for Health Care Providers, World Privacy Forum, 9/2008

Appendix C Health care providers may also be subject to the Address Discrepancy rules that apply to users of consumer reports. (A consumer report is also known as a *credit report*). A *Notice of Address Discrepancy* is a notice sent to a user by a consumer reporting agency (also known as a *credit bureau*) that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address in the agency's file for the consumer. 16 C.F.R. § 681.1(b). The Notice of Address Discrepancy is required by the Fair Credit Reporting Act. Under 15 U.S.C. § 1681c(h), when a person requests a nationwide credit report for a consumer, the request will include the address that the consumer provider to the person. If the address differs substantially from the address in the credit bureau files, the bureau notifies the requester of the existence of the discrepancy. The Notice of Address Discrepancy triggers obligations under the new rules. Any health care provider that orders a credit report on a consumer must comply with those obligations, which are discussed in more detail in section IV of this document. *Source: Red Flag and Address Discrepancy Requirements: Suggestions for Health Care Providers, World Privacy Forum, 9/2008*