



**Protecting Patient and Credit Privacy As  
Self-Pay Collections Move  
From the Back End to the Front End**

-----

**An nTelagent White Paper**

**[www.ntelagent.com](http://www.ntelagent.com)**

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

---

## Table of Contents

Background .....	3
Self-Pay Patients and Revenue Cycle Trends .....	4
Credit Score Limitations and Privacy Risks .....	5
Patient Access: Mission Control for Privacy Protection .....	7
Conclusion .....	9
About nTelagent, Inc. ....	10

## Background

Recently, a former national hospital chain employee was convicted of identity theft. The hospital chain acknowledged that the employee had access to the personal information of approximately 37,000 of its patients nationwide. The former employee had worked at the chain's billing office, which handles 4 million patient accounts. To help set things right, the company gave the 37,000 patients a warning that something might have happened to their data and set up a credit alert.

-----

In February 2008, security service provider SecureWorks reported an 85% increase in the number of attempted attacks directed toward its healthcare clients by Internet hackers. The firm noted that attempted attacks have increased from an average of 11,146 per healthcare client per day in the first half of 2007 to an average of 20,630 per healthcare client per day in the last half of 2007 through January 2008. Researchers report that one reason for the increase is the large amount of data healthcare organizations now hold in their systems: "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." (Source: *SecureWorks Threat Analysis, 2/13/08*)

-----

**The loss of privacy seems to many to be a foregone conclusion in the information age.** Americans are concerned about identity theft and fraudulent Internet deceptions. Recent "inside jobs" by healthcare employees, as well as an increase in attempted hacks on service providers, shine light on risks to patient data. Given current trends within the healthcare industry (discussed in the next section), as more and more data is collected from patients, providers must determine what type of information is most appropriate, and least vulnerable to attack. Systems to manage and protect the data must also be implemented to protect both the provider and the patient.

## Self-Pay Patients and Revenue Cycle Trends

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. With more and more patients entering healthcare facilities and emergency rooms as self-pay patients, however, **healthcare providers are facing the increasing challenge of collecting payments directly from the individual patients, who have assumed significant responsibility for paying for care.**

Self-pay is the portion of the medical bill for which the patient is responsible. This includes co-pays and deductibles for insured patients, and the full medical bill for uninsured patients. With the recent shift to consumer-driven healthcare plans and health savings accounts (HSAs), which carry significantly higher co-pays and deductibles than traditional insurance plans, a greater portion of self-pay accounts are derived from insured patients. Additionally, an increasing number of individuals with the financial capacity to purchase health

insurance are opting to “go bare” or without insurance.

In order to address this shift in collections structure, many healthcare facilities are concentrating on front-end collections to ensure timely and accurate payment from self-pay patients. **Patient privacy and data security is paramount in this environment**, as more demographic and financial information from patients is required upfront to establish financial responsibility, patient ability-to-pay, discounting, payment plans, charity care, assistance program eligibility and other assessments. Through all of these discussions, there is a need to monitor the patient payment metrics that matter most: what resources the individual and family have to pay for the healthcare they need.

*\*Editor’s note: For more information on front-end collections, download the white paper “From the Back to the Front: The Current Evolution of Healthcare Collections” on nTelagent’s website, [www.ntelagent.com](http://www.ntelagent.com).*

## Credit Score Limitations and Privacy Risks

**As the number of self-pay patients increases, healthcare providers will need to look for readily available methods that provide a complete, accurate picture of these patients' ability to pay for services.**

A *Wall Street Journal* article discusses the practice: "In a development that consumer groups say raises privacy issues, a growing number of hospitals are mining patients, personal financial information to figure out how likely they are to pay their bills. Some hospitals are peering into patients' credit reports, which contain information on people's lines of credit, debts and payment histories. ... Hospitals often use these services when patients are uninsured or have big out-of-pocket costs despite having health insurance. Hospitals say the practice helps them identify which patients to pursue actively for payment because they can afford to pay. They say it also allows them to figure out more quickly which patients are eligible for charity care or assistance programs. Administrators also argue that these credit checks can help them minimize losses. In 2006, nearly 5,000 community hospitals provided uncompensated care costing \$31.2 billion, the vast majority of it charity care or unpaid patient bills, according to the American Hospital Association." (Source: *Wall Street Journal*, "Why Hospitals Want Your Credit Report," 3/18/08)

A credit score is a number that represents an individual's credit worthiness. The score is based on a number that corresponds to an individual's credit report, including information such as payment history, amounts owed, and length of credit history, new credit and types of credit used.

Simply using a credit score to determine a patient's ability to pay, however, does not give a healthcare provider a complete or totally accurate picture. For example, hospitals and other caregivers already can tap into credit scores, but those are not necessarily a good indication of whether a patient will pay a medical bill. Credit scores are based on voluntary purchases, such as a car, and healthcare debt is largely involuntary. Other limitations, such as security freezes and state and federal legislation, are causing healthcare providers to look at other means of determining ability to pay.

Similar direction and benefits can be obtained by using available market data instead of credit data. Such an approach results in less risk of patient privacy being violated, as no credit card number or credit report data is stored.

**A comprehensive, effective self-pay management system offers healthcare providers the ability to determine capacity to pay at the point**

**of service, without using risky credit score/report information** -- allowing providers to assess more quickly which patients to pursue for payment because they can afford it, as well as which patients are eligible for charity care or assistance programs.

*\*Editor's note: For more information on credit scoring, download the white paper "The Limitations of Credit Scoring in Assessing Patients' Ability to Pay" on nTelagent's website, [www.ntelagent.com](http://www.ntelagent.com).*

## Patient Access: Mission Control for Privacy Protection

As hospitals and other providers seek to upend the revenue cycle status quo -- moving from back-end collections to front-end financial assessment and price transparency -- patient privacy and its protections under the Fair and Accurate Credit Transactions Act and other similar legislation need to be taken into consideration. Many providers are simply not prepared for the future -- especially in regard to patients paying an increasingly larger amount of their healthcare bill. **Concentrating on patient access basics and ways to ensure privacy protection within this area are critical.**

The battle to include patient access staff (e.g., admissions and registration) as part of the revenue cycle is largely over. It is well-known that gathering demographic information and billing information at the time of registration and/or scheduling is essential to creating appropriate billing practices (including cleaner claims).

Disagreement arises on how best to incorporate patient access management into the revenue cycle. Some organizations focus on retraining staff and requiring them to collect more information; others invest in technology to automate processes. Many choose a combination of the two. Access management basics include:

- **Embedding insurance eligibility into patient access workflow.** Verifying eligibility at the time of registration removes one more opportunity for human error in the process. Lack of insurance coverage can trigger charity care and discounting.
- **Embedding rules to guide registrars.** Registrars and financial counselors should be supported with automated rules and scripts requiring that certain pieces of information be gathered before proceeding with registration. Security levels and access to information should be determined based on patient type and collection business rules.
- **Verifying patient addresses.** Verifying patient mailing addresses should be an integrated step in patient access workflow, with the address check being performed as the registrar types in the patient address. This is especially important as the self-pay portion of healthcare continues to increase.

**In the age of healthcare consumerism, the demand for improved service begins in the patient access area. Privacy protection can be a differentiator.** Patient privacy practices must be

observed at each point in the patient access process, including:

- Non-credit demographic access
- Demographic profiling
- Insurance verification
- Charity documentation
- Price transparency
- Patient registration
- Government program eligibility

In all of these steps, the security of information can be enhanced by using market data (e.g., publicly available demographic information) -- rather than credit data that include Social Security

numbers, credit card numbers and credit scores.

Finally, to allay concerns that patient financial information could be used to determine clinical treatment, a web-based demographic solution as part of a self-pay management system can be implemented. Such a solution is used for financial determinations only and stands alone from the clinical system.

## Conclusion

Patient privacy concerns are at the forefront as the need for financial information at the point of service is increasing. The looming question is the degree to which patient confidentiality can be protected -- at the same time more information is needed about an individual's capacity to pay -- both for service provider collections and charity care documentation.

One approach many providers are adopting is the use of available market/ demographic data, instead of keeping credit card numbers and report data on file. **Using non-credit data as a basis for collecting patient demographic information protects the patient from identity theft.** This approach also decreases the likelihood that patient access staff members or other employees would be tempted -- or able - - to use the data inappropriately.

In summary, a self-pay management system should move beyond obtaining a credit score to establishing an economic profile of the patient via the assimilation

of demographic data. According to one healthcare executive: "We do not use a credit score to determine an individual's ability to pay simply because our system's algorithm can be more accurate and does not hold the liability that goes along with obtaining credit scores."

Ultimately, patient security is achieved by the following variables within an organization:

- Leadership and commitment
- Culture
- Resource capacity and competency
- Process and outcomes
- Data assessment
- Operational efficiency
- Communication

## 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](http://www.ntelagent.com) for more information.