

Protecting Patient Privacy

Data security and front-end collection of patient-responsible balances

Healthcare Registration, by Irene Barron, June 2011

Security service provider SecureWorks recently reported that attempted hacker attacks launched against health care clients nearly doubled during the last quarter of 2009.

The firm noted that attempted attacks rose from an average of 6,587 per health care client per day during the first nine months of 2009 to an average of 13,379 attacks per client per day in the last three months of 2009. Researchers report that one reason for the increase is the large amount of data health care organizations now hold in their systems -- “veritable treasure troves of sensitive data.”ⁱ

“Health care organizations often store valuable data such as a patient’s Social Security number, insurance and/or financial account data, birth date, name, billing address, and phone, making them a desirable target to cyber criminals,” SecureWorks noted in a press release.ⁱⁱ

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 health care employees, as well as an increase in attempted hacks on service providers, shine light on risks to patient data.

Given current trends within the health care industry, 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 data also must be implemented to protect both the provider and the patient.

Patient Information and Revenue Cycle Trends

Since the advent of health insurance options, including private insurance, Medicare and Medicaid, the focus of collections for health care service providers has been on the back end. Today, however, health care providers are facing the increasing challenge of collecting payments directly from individual patients, who have assumed significant responsibility for paying for their medical care.

With the recent shift to consumer-driven health care plans and health savings accounts, which carry significantly higher copays and deductibles than traditional insurance plans, a greater portion of patient-responsible balances are derived from insured patients. This shift has been compounded as insurance payors, in response to the passage of health care reform, continue to raise patients’ deductibles and coinsurance amounts. In addition, 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 health care facilities are concentrating on front-end collections to ensure timely and accurate payment from 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, financial assistance program eligibility and other assessments.

Credit Score Limitations and Privacy Risks

Health care providers need to look for readily available methods that provide a complete, accurate picture of patients' ability to pay for services -- and they must do so while ensuring and protecting patient privacy. As noted in a *Wall Street Journal* article:ⁱⁱⁱ

“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.”

A credit score is a measurement based on an individual's financial history (e.g., payment history, amounts owed, 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 health care 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. The reason: Credit scores are based on voluntary purchases, such as a car. Health care debt, however, is largely involuntary.

Other limitations, such as credit freezes and state and federal legislation, are causing health care providers to look at other means of determining ability to pay. Similar direction and benefits can be obtained by using publicly available demographic data instead of credit data. Tapping these other resources allows health care organizations to take an approach that results in less risk of patient privacy being violated, as no credit card number or credit report data is stored.

A comprehensive, effective point-of-service system offers health care providers the ability to determine capacity to pay upfront, without using risky credit score/report information. This allows providers to assess more quickly a patient's financial responsibility based on capacity to pay, as well as determine which patients are eligible for financial assistance programs.

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 -- patient privacy and its protections under the Fair and Accurate Credit Transactions Act and similar legislation need to be taken into consideration.

Many providers simply are not prepared -- especially in regard to patients paying an increasingly larger amount of their health care bill. Concentrating on patient access basics and ways to ensure privacy protection within this area are critical.

The battle about the need to include patient access staff, at admissions and registration, as part of the revenue cycle is largely over. It is well known that gathering patient demographic information and billing information at the time of registration and/or scheduling is essential to collecting patient-due portions effectively, to generating cleaner claims and to controlling bad debt.

Issues sometimes arise, however, 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 financial assistance and discounting.

Providing rules to guide patient access employees. Front-end employees 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 identity. Verifying patient identity (knowing for sure that the patient is who he says he is) should be an integrated step in patient access workflow.

Estimating patient-balance due. Providing the registrar with tools to determine the amount to be collected along with financial assistance options is critical in order for front-end collections to be successful.

Patient Privacy at Access

In an age of health care 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:

- capacity-to-pay determination based on demographic information,
- insurance and identity/address verification,
- financial assistance documentation,
- patient-balance estimates based on contract terms, and
- government program eligibility.

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

In Summary

Patient privacy and confidentiality must be protected as the need for financial information at point of service is increasing. A point-of-service system should move beyond obtaining a credit score to establish an individual's ability to pay. One approach many providers are adopting is the use of publicly available demographic data, instead of keeping credit card numbers and credit report data on file.

Using non-credit data 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 patient data inappropriately.

As one health care executive notes, "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."

Reader's Resource

This article is excerpted and reprinted with permission from nTelagent, which offers a total point-of-service solution for the health care industry. For more information, go to ntelagent.com.

ⁱ Accessed 5/19/11: <http://www.secureworks.com/research/newsletter/2010-01/>

ⁱⁱ Accessed 5/19/11: http://www.secureworks.com/media/press_releases/PR/13571/

ⁱⁱⁱ Accessed 5/19/11: <http://online.wsj.com/article/SB120580305267343947.html>