White Paper

The Real Cost of Health Care Fraud – and New Ways to Fight It

Stopping the Flow of Health Care Fraud with Technology, Data and Analytics

January 2014

LexisNexis®

Risk Solutions
Health Care

Health care costs are rising and everyone is being affected, including patients, providers, insurance companies and other organizations. While many efforts have been made to control those costs, including the federal government's health care reform law, the Patient Protection and Affordable Care Act, many observers say efforts haven't gone far enough in solving one of the top problems in medicine today: health care fraud.

A growing problem

The FBI estimates that between 3% and 10% of all health care spending in the U.S. goes toward fraudulent claims. In other words, anywhere from $70 billion to more than $200 billion per year is lost because of health care fraud, says the National Health Care Anti-Fraud Association[1].

In 2010 alone, Medicare and Medicaid made more than $68 billion in improper payments, according to an estimate from the Government Accountability Office[2]. And while the government is a big target for fraud, private insurers are subject to the same risk.

As the money spent on health care continues to rise, the impact is only going to grow. More and more criminal organizations are targeting the health care industry, especially as greater use of electronic records and other health IT makes it easier for those groups to steal data to commit medical identity theft and other scams.

Rising costs will also likely lead to an increase in more subtle forms of illicit activity, as doctors and patients try to supplement income and cut their own expenses.

Fraud, waste and abuse

While there are some dishonest providers and organized crime groups that run sophisticated scams, the problem comes in many different forms. Activity payers need to look out for comes in three broad categories:

- **Fraud** – This is when an individual or organization intentionally falsifies information for financial gain. One of the most common examples is a provider submitting claims to a payer for services that were never performed. Other types of fraud include "upcoding," in which the provider bills for a higher CPT code than what was actually performed, and billing separately for services that should have been bundled together and billed at a lower cost. Fraud also occurs on the patient side, such as when an individual uses another person's insurance to receive care, or visits multiple doctors to obtain unnecessary prescriptions for drugs.

The FBI estimates that between 3% and 10% of all health care spending in the U.S. goes toward fraudulent claims

[1] http://www.nhcaa.org/media/5994/whitepaper_oct10.pdf
[2] http://www.gao.gov/new.items/d11409t.pdf

- **Abuse** – Abuse is similar to fraud, except it refers to cases in which criminal intent can't be proven. It might occur when providers accidentally overcharge for services or use an incorrect code. While the law distinguishes between fraud and abuse, the end result to payers is the same – the organization ends up paying money for something that shouldn't have been reimbursed.
- **Waste** – This is what happens when providers misuse resources, which can occur intentionally or unintentionally. One example is writing prescriptions for expensive medications when low-cost generic alternatives are available. On the more dangerous side are the examples of doctors performing inappropriate or unnecessary procedures.

Lives could be at stake

It's not just insurers' bottom lines – and, due to a trickle-down effect, patients' wallets – that are being affected. Health care fraud has real and serious consequences on the quality of care.

Of course, performing unnecessary medical services is bad for a patient's health. But all types of fraud, waste and abuse can lead to dangerous or even deadly results.

For example, when providers commit fraud by submitting false claims to payers, they have to alter patients' records to support those claims. If that's never corrected, it means the patient's medical history is inaccurate, which could lead to an incorrect diagnosis or treatment in the future.

It could also become difficult for that person to get insurance coverage down the road, or add to the patient's premiums.

Victims of medical identity theft also face some dangerous consequences, according to a 2012 survey from the Ponemon Institute[3]. Among 807 patients who were affected by medical identity theft:

- 41% were terminated by a health plan or provider
- 30% had to spend significant time clearing up inaccuracies in their medical records
- 14% received incorrect treatments because of those inaccuracies, and
- 12% were diagnosed incorrectly as a result.

[3] http://www.ponemon.org/local/upload/file/Third_Annual_Survey_on_Medical_Identity_Theft_FINAL.pdf

It's not just insurers' bottom lines – and, due to a trickle-down effect, patients' wallets – that are being affected. Health care fraud has real and serious consequences on the quality of care.

Improper claims caught too late

The really bad news is that the majority of health care fraud, waste and abuse is never caught, meaning those claims end up being paid, along with all of the negative consequences for patients.

Part of the reason is that the wide variety of dishonest or wasteful claims makes them hard for payers to catch, since the activity doesn't always have clear warning signs. That's becoming even more of a problem as criminals are developing more sophisticated methods to defraud payers while avoiding detection.

As a result, the majority of payers are stuck focusing on tracking down fraud after the claims have been paid, as opposed to detecting it in the prepayment stages. And anyone involved in finance knows that once money leaves the organization, it's very difficult to get it back.

But unfortunately, that's the way it normally happens for all types of fraud, waste and abuse. For example, in the Ponemon survey of patients who knew they had been victims of medical identity theft, most only found out after the fact.

In fact, only 4% of the respondents were notified of the fraud by their insurance company, while 10% learned from their health care provider. Victims were more likely to find out through other means:

- 39% discovered the fraud after getting collection letters seeking their out-of-pocket portion of the claim
- 32% learned of the incident because of mistakes in their medical records
- 26% first noticed suspicious items on statements or invoices, and
- 15% found adverse entries on their credit report.

Find fraud before claims are paid

Often if a claim is paid, it's too late for the payer to recover its losses. It's also difficult for the affected patients to get everything straightened out on their end.

And only a small portion of those claims are even spotted – it's all the fraud, waste and abuse that goes completely undetected that has the most serious impact.

The only real way to prevent a fraudulent act is to stop it in its tracks – before payment.

Of course, investigating every claim before it's paid would be impossible for payers. That's why many payers are turning to tech tools to help weed out the inappropriate claims so they can quickly and efficiently pay the claims that are legitimate.

Part of the reason is that the wide variety of dishonest or wasteful claims makes them hard for payers to catch, since the activity doesn't always have clear warning signs.

New data analysis tools

While more information going digital can in some ways help criminals carry out their scams, the good news is that health care firms have access to more data than ever. When used the right way, that information can help root out fraud, waste and abuse.

Analyzing data, including public records, online information and data from the payer's own transactions, can provide an effective way to catch suspicious claims or patterns of behavior.

Here are some of the options made available by evolving technology systems:

1. Rules engines

One goal payers have is to catch claims that go against their policies. Many firms also flag certain transactions as needing closer inspection, such as those that exceed certain dollar amounts.

Fraud detection systems with rules engines allow payers to define rules so that the software automatically notifies staff to take a closer look.

Many types of suspicious activity can be caught by checking claims against those rules. For example, a system might red-flag a claim if a provider is claiming to perform the same services for multiple family members within a short time period. A rules engine can also find out if a claim is inconsistent with the patient's previous history, which is another common sign of fraud.

2. Data analytics

The disadvantage of relying on a rules-based system is that payers must set those rules ahead of time – so only previously known fraud patterns will be caught.

But as more information becomes available, systems are becoming more sophisticated and able to mine that data to find claims that are out of step with normal activity. That can greatly improve a payer's ability to detect inappropriate claims or to identify providers with a pattern of suspicious behavior.

For example, a system can look at a provider's total charges per visit, number of weekly patient visits and other metrics, and compare them to averages for all similar providers. Anything that's significantly out of line could be a big warning sign.

So-called "predictive analytics" are a big component in the federal government's fight against Medicare fraud, which resulted in the recovery of $4.2 billion in 2012[4].

Analyzing data, including public records, online information and data from the payer's own transactions, can provide an effective way to catch suspicious claims or patterns of behavior.

[4] http://www.hhs.gov/news/press/2013pres/02/20130211a.html

3. Identity verification

One important part of weeding out fraudulent claims is verifying that the parties involved are who they say they are. In addition to medical identity theft, some forms of fraud involve doctors lying about their credentials to file claims.

Advanced systems can verify the identities and credentials of doctors and patients by checking information from claims against public records databases to check for any discrepancies. Those checks can also reveal red flags in individuals' backgrounds, such as prior fraud accusations and legal charges in other states.

4. Social network analytics

In addition to all the new digital information created in health care settings, there's a lot of information in general available on the Internet – with much of it being uploaded by individuals themselves on social networking sites.

Many fraud prevention systems are now using that data to find information that might help uncover suspicious claims activity. Health care fraud is often carried out by teams – for example, a provider might recruit patients to act as accomplices and allow their records to be used to submit false claims. In many cases, those scams are perpetrated by people with pre-existing relationships.

By analyzing data from social networks, fraud detection systems can see if individuals have any connections with known or suspected fraudsters, or find connections between patients and the doctors and other employees of the providers filing the claims. That can help determine which claims might warrant closer inspection.

Conclusion

As criminals and scammers get more sophisticated, payers must do the same so they can stop healthcare fraud before claims are paid.

Not only will that save payers a lot of money, but reducing fraud, waste and abuse will also lead to lower costs throughout the healthcare system and help avoid serious problems for patients.

As criminals and scammers get more sophisticated, payers must do the same so they can stop health care fraud before claims are paid.

For more information:

Call 866.242.1442 or visit
www.lexisnexis.com/risk/healthcare

About LexisNexis® Risk Solutions

LexisNexis® Risk Solutions (www.lexisnexis.com/risk/) is a leader in providing essential information that helps customers across all industries and government predict, assess and manage risk. Combining high-performance cluster computing, unparalleled stores of public data and social networking and predictive analytics, we provide products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of Reed Elsevier, a leading publisher and information provider that serves customers in more than 100 countries with more than 30,000 employees worldwide. Our health care solutions assist payers, providers and business partners with ensuring appropriate access to health care data and programs, enhancing disease management contact ratios, improving operational processes and proactively combating fraud, waste and abuse across the continuum.