White Paper

Advanced Data and Analytics for Property Casualty Insurance—the Cure for the Medical Provider Claims Fraud, Waste and Abuse Epidemic

June 2015

LexisNexis®

Risk Solutions
Insurance

Executive Summary

Annual losses from medical claims fraud, waste and abuse are now in the hundreds of billions of dollars. Furthermore, over 80% of medical claims fraud is suspected, at varying degrees, to involve medical providers. This population represents the largest problem area, but also the greatest opportunity to impact and reduce medical fraud, waste and abuse losses. This problem will continue to grow for property casualty insurers as managed healthcare forces many doctors to find new ways to make money. While it may seem like a battle that can't be won, access to more comprehensive data, and the technology to interpret the data, offers new hope for the property casualty insurance industry. Innovation has produced a viable fraud defense system capable of turning the tides of medical claims fraud and drastically reducing its devastating losses.

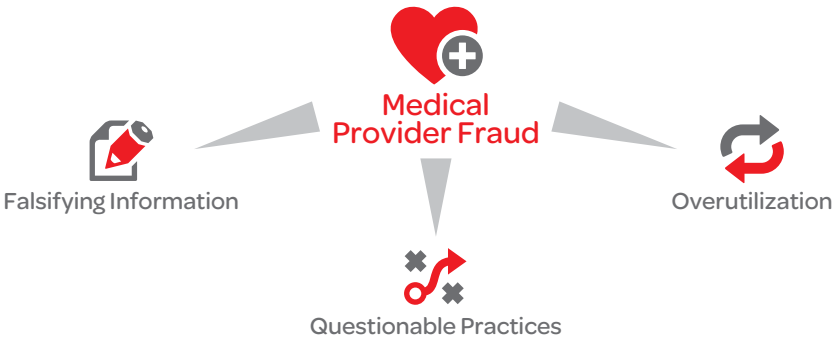
The problem: Three core types of medical claims fraud seen by property casualty insurers

A prerequisite for stopping fraud is having a clear understanding of the types of fraud that are being committed and the methods being used to get away with it. There are countless tactics that fraudsters are using, but most, if not all, fall into one of three main categories:

1. **Falsifying information:** This includes tactics like fake coding and altered claims and often involves patients that don't actually exist and/or billing for services that were never rendered. This is the least common of the three main fraud types and represents the smallest percentage of losses associated with fraud and abuse.

2. **Questionable practices:** This includes tactics such as upcoding, unbundling, cost shifting, over or mis-prescribing, clustering, underutilization, invalid service locations and non-contracted providers. This type of fraud is very common, results in a large percentage of total medical claims fraud losses, and has historically been very difficult to detect.

3. **Overutilization:** This type of fraud is the largest cause of losses and is also the most difficult to detect. It includes activities like: intentional misdiagnoses, unnecessary treatments and procedures, unnecessary durable equipment and inflated visit frequency.



A problem of epidemic proportions

"The **units of measure for losses due to health care fraud and abuse in this country are hundreds of billions of dollars per year.** We just don't know the first digit. It might be as low as one hundred billion. More likely two or three. Possibly four or five. But whatever that first digit is, it has **eleven zeroes after it**."[1]

The inadequacies of a bill-level fraud prevention strategy

For most property casualty insurance companies the traditional method of attempting to identify and prevent fraud solely by reviewing individual bills is woefully inadequate for a variety of reasons:

- This myopic perspective only sees a single, isolated claim at one point in time—with no historical or relational context.
- Reviewing every bill manually, without the support of data analysis, often fails to reveal more subtle indicators of fraud.
- Fraud indicators on a single bill provide no evidence of a recurring pattern and can be easily shrugged off as human error.
- Bill review rules can be easily learned and exploited by practitioners.

Evolving to a provider-level strategy

Instead of looking at individual bills as they come in, technology enables carriers to access a broad range of intelligence based on years of data related to providers, their practices and their claims histories. Instead of the narrow view offered by using only limited provider data, leading solutions deliver a big-picture view of providers made possible by leveraging many other types of data about them. This high-definition, provider-level perspective is available today, and it is more comprehensive, holistic and insightful. The provider-level perspective reveals patterns that are impossible to recognize from the bill-level point-of-view.

This provider-level approach involves processing massive amounts of data from multiple sources (both intra-industry and cross industry databases) and also uses advanced analytic models to complete a three-stage process that results in a highly effective fraud detection and prevention solution:

Stage 1: Provider resolution

By overlaying and comparing data from various sources, advanced linking technology can quickly verify and confirm valid provider identities and recognize anomalies that suggest errors or intentionally falsified identity data. Provider resolution involves recognizing and linking all the identification information associated with a particular provider, generating the most comprehensive, multi-layered view of that provider. Stage one answers the question, "Which identity information belongs to this particular provider?"

Stage 2: Providers of interest identification

Property-casualty focused analytic models are designed to recognize a wide variety of factors that are known indicators of medical claims fraud. Data intelligence can flag instances in which a provider is known to have previously committed a non-medical type of fraud such as financial or tax fraud. Or, the analytics may reveal suspicious patterns in a provider's medical claims. Most models will also provide scoring mechanisms based on the likelihood of the presence of fraud and the seriousness or scope of the fraudulent activity. Stage two answers the question, "Does this provider warrant further investigation?"

Stage 3: Investigation and evidence building

Once the "providers of interest" have been identified and prioritized, today's analytic tools enable users to easily monitor suspicious providers and dig deeper to conduct thorough investigations. Information that previously took weeks or months to gather and analyze can now be delivered and actionable in seconds. Armed with this technology, property casualty insurers are able to more effectively allocate resources and efficiently gather evidence to prove medical claims fraud. Finally, insurance organizations can position themselves to make real progress in the battle against fraud.

Provider-Level Three-Stage Fraud Detection and Prevention

Stage 1: Provider resolution

Recognize and link all identification information to a provider

Stage 2: Providers of interest identification

Flag providers that warrant further investigation

Stage 3: Investigation and evidence building

Monitor suspicious providers and gather evidence

Where should the data come from?

One of the key reasons that this innovative provider-level strategy would be so powerful and effective is that the data that fuels the solution would come from so many different sources. Using data from multiple resources provides a multi-dimensional perspective of providers. This aggregation of different types of information enables users to see more—and to see more clearly. So, where should the data come from?

- **Intra-industry contributory data:** This is the specific provider claims data that most insurance carriers submit to the industry's contributory database.
- **Cross-industry contributory data:** This includes contributory data from sources other than medical claims, including: healthcare, government, financial services and workers' compensation.
- **Public records data:** This includes identification data, like name, phone number, address and SSN, as well as other "footprint" data, like bankruptcies, deceased files, watchlists, criminal records, etc.

Transforming data into intelligence with analytics

Having data is useless without the means to derive and understand insights from it. Let's take a more detailed look at the three stages of provider-level fraud prevention to see how raw data becomes actionable intelligence.

Provider resolution

Providers with the intent to commit fraud will frequently create false identities or even use deceased identities, which are then used to submit false claims. In addition, many legitimate, lawful medical service providers may work out of multiple locations, which means they may have multiple phone numbers and addresses. This can make it difficult to reconcile some provider identities.

Provider resolution example

In a real world scenario, a data file with over 450,000 provider identities was processed through a quality identity resolution solution. The results showed that the 450,000 identities actually belonged to only a little over 250,000 unique providers. And 400 of the providers were making claims under identities of deceased individuals.

Today's identity resolution solutions use advanced data matching, linking and relationship mapping to recognize dissimilar identification information that's linked to a single individual. While some dissimilar information can be attributed to legitimate reasons or accidental errors, many of the anomalies are indicators of intentional fraud.

Identifying providers of interest

One of the most effective new methods for revealing fraudulent medical claims practices is peer comparison analytics. By comparing a single provider's claims history to industry standards and averages (for that particular specialty), unusual activities and patterns can be easily recognized and flagged. Peer comparison predictive models leverage many different types of data, for example:

- **Time-based profiles:** Are the minutes and hours being charged for certain procedures in line with the typical amount of time associated with those procedures? And are the procedures being done at unusual times or on weekends and holidays?
- **Procedure codes:** Is this specialist performing procedures that are unusual or performing them with unusual frequency?
- **Diagnostic codes:** Is the specialist diagnosing certain injuries with unusual frequency?
- **Treatments:** Is the provider prescribing treatments that are inappropriate for the diagnosis?

As previously mentioned, once the analytics are complete the model assigns a score based on the probability that a provider is committing fraud and the predicted severity of the provider's activities. Armed with this prioritized list, a carrier would then be empowered to make informed decisions about allocating resources for further investigation and evidence gathering.

Drilling down to the proof

Today's medical claims fraud solutions can do more than detect probable fraud. They can also help carriers monitor and investigate suspicious providers in order to compile solid evidence and proof of fraud—and ultimately help carriers stop fraudsters in their tracks. Here are a few specific tactics that can be deployed at this stage:

- **Monitoring:** Place providers of interest on external watchlists and flag them for ongoing internal claims monitoring. With provider-level intel, you can now go back and monitor providers of interest at the bill level with an appropriate level of discretion. You can proactively track outlier activities and ensure adherence to regulations and business rules.
- **Investigation:** Integrate public records data in order to see the provider and the person. Public records data can offer insights into a person's character,

Today's medical claims fraud solutions can do more than detect probable fraud. They can also help carriers monitor and investigate suspicious providers in order to compile solid evidence and proof of fraud—and ultimately help carriers stop fraudsters in their tracks.

behavior and even motivations for attempting fraud. For example, public records may reveal that a provider:

- Just filed bankruptcy – may indicate personal and/or professional financial strain
- Owns a company being sued for fraud – may indicate a pattern of behavior
- Has moved three times in five years – may indicate instability, reputational or legal problems
- Has multiple IDs linked to different practices – may indicate the intent to commit fraud

- **Action:** Once you've completed investigations, you're in a position to take informed action based on the circumstances of each case.
  - Honest providers will likely correct unintentional mistakes
  - Some dishonest providers will correct their behavior once they realize they've been caught
  - Serious fraudsters will either keep trying new fraud methods or abandon their carrier for another when they realize they can't get away with fraud
  - High-profile and clear black-and-white cases of fraud may be turned over to law enforcement for prosecution. Other cases may simply require carrier confrontation

Getting started

The best news about the evolution of the war against fraud is not only that there is powerful new technology to help in the cause, but also that this new approach is easy and affordable to implement. Here are a few simple steps to help your organization get started:

1. Inquire about LexisNexis Risk Solutions data analytics tools that enable the shift from a bill-level to a provider-level strategy

2. Use those tools to identify and prioritize providers of interest and then to prove which ones are fraudsters

3. Fight fraud or at least negotiate better settlements

4. Expand and adjust your solution as needs dictate

Fraudulent medical providers have been milking the system for years. The hundreds of billions of dollars lost to fraud, waste and abuse every year are a major contributor to skyrocketing medical costs. Medical claims fraud is an inexcusable crime with far-reaching consequences. Up until now, fighting it has been a losing battle—but now carriers can arm themselves with data and analytics technology that gives them the advantage. Now carriers turn the tides and substantially reduce fraud losses.

About the Authors

Todd Fannin is Director, Vertical Markets, for the risk solutions business of LexisNexis.® He is responsible for gathering market feedback from customers and prospects, then working with the LexisNexis product development team to create the solutions that help customers improve claims workflow processes and manage their bottom line. He joined LexisNexis in January 2012. Previously, Fannin served as director of both technology and the claims process at Esurance. He also served as manager of the company's claims process. Fannin earned his Bachelor's Degree in Accounting from Shorter College.

Shannon Holt is Senior Product Manager, Analytics Products, for the risk solutions business of LexisNexis.® She is responsible for driving the definition and execution of auto claims product plans from concept development through market launch and product support once in production. Previously, Holt owned a consulting firm that provided risk management services including claim history analysis, claims handling standards development and incident investigation. Holt earned her Bachelor's Degree in Risk Management and Insurance from Florida State University.

For more information:

Call 800.458.9197 or email
insurance.sales@lexisnexis.com

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 cutting-edge technology, unique data and advanced scoring 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 insurance solutions assist insurers with automating and improving the performance of critical workflow processes to reduce expenses, improve service and position customers for growth.

LexisNexis®

[1] Malcolm K. Sparrow, Professor of the Practice of Public Management, John F. Kennedy School of Government, Harvard University; author "License to Steal"; May 20, 2009 testimony before the United States Senate Committee on the Judiciary: Subcommittee on Crime and Drugs.