White Paper

Key Factors for Payers in Fraud and Abuse Prevention

Protect against fraud and abuse with a multi-layered approach to claims management.

October 2012

LexisNexis®

Risk Solutions
Health Care

Whether an act is technically labeled "health insurance fraud" or "health insurance abuse", the impact can be equally profound, with payers standing to lose money and patients put at financial and physical risk.

Overview

From individuals sharing their health insurance cards for use by family or friends who do not have coverage, to unethical providers billing for services never rendered, to sophisticated criminal rings, today's payers are at war with perpetrators of false and intentionally inaccurate claims. To win this conflict, they must arm themselves with the tools necessary to detect and prevent fraud and abuse and accurately validate charges prior to issuing payment without disrupting the payment process for honest claimants.

Further, tactics to prevent health insurance fraud and abuse cannot stand alone, but must be integrated into operations in a manner that:

- Ensures secure information management
- Contains costs
- Enhances operational efficiency
- Improves investigative efficiency
- Minimizes false-positive results
- Promotes compliance with global regulations

It is a daunting task. However, it can be accomplished. By focusing on five key factors, payers can take the offensive in combating health insurance fraud and abuse, building toward a complete and comprehensive solution.

Step 1: Data

Making the best use of information

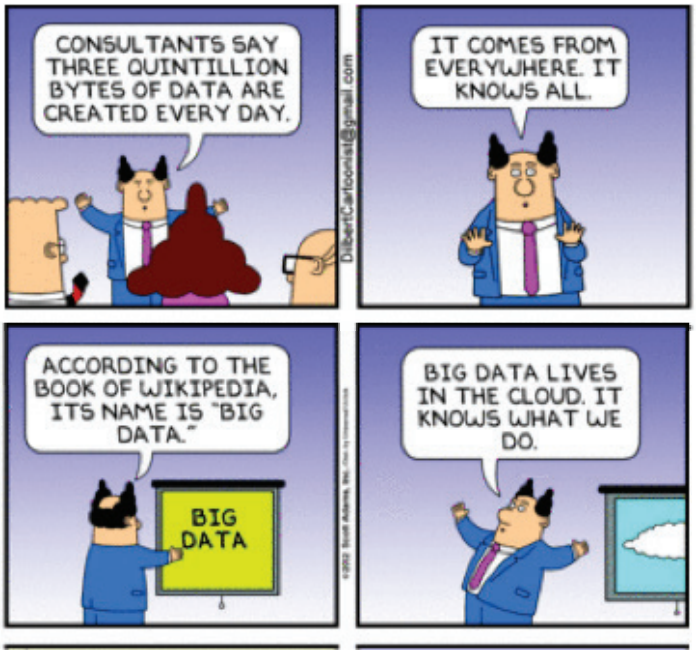
Payers' processes are data driven. Databases must be as accurate and up-to-date as possible, and the depth and breadth of information available must be sufficient to help them make the best decisions.

A recent development among health insurers is the stated goal of moving from fraud and abuse detection to prevention, taking action before a claim is paid and putting an end to what is frequently referred to as our historical pay-and-chase approach to fraud and abuse

At LexisNexis, we believe achievement of that objective rests on real-time access to vast and diverse information sources, integrating internal and external information to put the spotlight on malfeasance and misrepresentation. This process has been referred to as harnessing the power of so-called "big data," a concept that is well recognized in other industries but relatively new to health insurance.

When claims data is juxtaposed with other information, including external data such as public records, a more complete and accurate picture of an individual or organization is revealed.

The term "big data" was originally coined to describe the immense amounts of data that collect over time and are difficult to analyze and administer using common database management tools. Advances in super-computing, analytics and data storage capacity, however, are changing that definition, leading to the July 29, 2012, "Dilbert" cartoon highlighted below.



Yes, it does, and it knows things payers must know about their members, providers and suppliers to operate in the most efficient and effective way, from up-to-date contact information to "hidden" relationships between individuals and between individuals and businesses to possible derogatory indicators.

When claims data is juxtaposed with other information, including external data such as public records, a more complete and accurate picture of an individual or organization is revealed. This enables payers to conduct fact-finding research, due diligence and fraud investigations more efficiently and cost effectively.

Step 2: Identity Management

Knowing with whom, you are dealing

Medical identity theft continues to rise. According to the Ponemon Institute, an estimated 1.85 million Americans were affected in FY 2012 vs. 1.49 in FY 2011. The consequences for victims is deep and wide, from loss of benefits and lowering of credit scores to erroneous information making

. . . it's not just the patients; providers also may not be who —or what—you think they are.

its way into the victim's medical records, potentially jeopardizing their health and possibly even their life.

This type of fraud continues to be what Ponemon calls "a family affair". 36 percent of those surveyed said a member of their family took their personal health identification credentials, such as their insurance card, without their knowledge and 31 percent said they willingly shared their personal identification information with a family member who did not have health insurance in order for them to obtain medical services.

Medical identity theft also can be an "inside job," with employees channeling information to individuals for personal use and organized rings for sale on the street or use in elaborate fraud schemes.

And it's not just the patients; providers also may not be who – or what – you think they are.

For instance, could there be providers in your network practicing with an expired license? Have any of them previously been convicted of a felony? Do they really have the credentials they claim? Have they been barred from participating in other programs or networks due to fraudulent acts?

The correct answers to those, and similar, questions are of great import to protecting both patient safety and payer solvency.

Today, there are tools available to access and analyze the breadth of information payers need to accurately identify providers. Industry-leading tools also enable actionable insight into the risk associated with would-be providers before the relationship is formalized and system access is granted.

Payers can further enhance provider enrollment through credential verification, background evaluation and ongoing alerts to derogatory indicators and adverse changes, while ensuring members continue to meet eligibility requirements.In this instance, it's not a matter of who you know that counts, but, rather, what you know about them.

Step 3: Predictive analytics

As noted, payers traditionally have relied on post-payment claims solutions, cutting checks and then attempting to recover funds found to have been paid in error or tied to fraud or abuse.

Today, forward-thinking payers are taking a multi-layered approach that uses predictive analytics and sophisticated modeling capabilities to

. . . it's not a matter of who you know that counts, but, rather, what you know about them.

identify fraud and abuse patterns and risk indicators as they emerge – and before a claim is paid.

Moving detection to the front end of the claims payment process and complementing it with predictive modeling techniques can tilt the scales to payers' advantage, allowing them to mitigate fraudulent and abusive actions while paying legitimate claims as efficiently as possible.

Predictive analytics have leapfrogged the traditional rules-based method, applying algorithms that identify abnormalities not immediately apparent by other means. Considering multiple factors too subtle or complex for traditional rules-based applications to identify, predictive modeling also is capable of "learning through experience."

The more information the model can collect, the more powerful it will be. Thus, predictive analytics takes fraud and abuse prevention yet another step further, using big data not just to authenticate and validate individual identities but to predict their future behavior vis a vis claims.

Step 4: Social network analytics

Late last year, a report was released suggesting that the concept of "six degrees of separation" was invalid and that, indeed, the average number of acquaintances separating any two people in the world was actually 4.74.

Whatever the number, the point is clear: People are connected through complex, intersecting clusters of relationships. In the context of fraud and abuse, finding those clusters and dissecting them with social network analytics can yield valuable information for payers.

This dissection is becoming easier with the advent of highly sophisticated social networking analytics processes, which allow users to measure and map the flow of relationships and relationship changes between knowledge-possessing entities.

Social network analytics provide a different kind of data mining, summarized with graphing – a visualization tool that makes significant connections among individuals and behaviors clearer and that correlates relationships between entities that would otherwise go undetected.

The best applications of social network analytics put intelligence gathering in a relationship context that highlights associated risk, displaying the degree of association and confidence in each linkage and other information that could prove valuable to research and investigations. Like the factors above it, though, social network analysis can't shoulder the

The best applications of social network analytics put intelligence gathering in a relationship context that highlights associated risk .

fraud-prevention burden alone. It is essential to have powerful technology that can take all the bits and bytes of social network analytics findings and put them together in a meaningful way.

Step 5: Linking technology

Yes, even if payers have the right amount of correct – and right – data, a secure and optimized identity management process and both predictive and social networking analytics in place, they still need a way to make them function as integrated parts of a whole rather than individual solutions that are independent of one another.

That's where advanced linking technology comes into play, turning disparate data into actionable information.

The fact is that as health care data becomes more complex and fraud schemes more sophisticated, traditional linking technologies are no longer capable of doing the job. This is because those legacy systems are limited by the methods and data used to accomplish linking, generally relying on characteristics that frequently change (such as addresses and phone numbers) and are not clearly disambiguated enough to ensure against false positives.

Today's truly advanced linking technology utilizes a unique and persistent identifier that guards against false positives, providing more precise, relevant information in less time.

Far more powerful than its predecessors, state-of-the-art linking technology is capable of intelligently analyzing billions of records to identify, analyze, link and organize information quickly and accurately for optimal results.

Conclusion

Medical fraud and abuse is a serious and complex problem in the United States. To effectively protect themselves and their participants against health care fraud and abuse, health plans must put in a place a tiered approach that incorporates both the greatest amount of data possible and the tools needed to bring information imbedded in that data to its essence quickly, effectively and efficiently.

The fact is that as health care data becomes more complex and fraud schemes more sophisticated traditional linking technologies no longer are capable of doing the job.

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.