White Paper

Bending the Cost Curve: Analytics-Driven Enterprise Fraud Control

Three percent, or $60 billion, of all health care spending is lost to fraud.

April 2011

LexisNexis® | Health Care

Introduction

The United States now spends about $2.6 trillion annually on health care (17.5% of GDP). With the proposed reform initiatives under the Affordable Care Act (ACA), the number of Americans covered and the amount spent will grow dramatically, potentially leading to even greater fraud, waste and abuse in the system.[1] Health care fraud is a national problem, prevalent in federal, state and private insurance programs. In the U. S., health care fraud has skyrocketed over the last decade, with billions of dollars being paid on improper claims.[2] The National Health Care Anti- Fraud Association (NHCAA) conservatively estimates that 3 percent of all health care spending, or $60 billion, is lost to health care fraud.[3] Other estimates[4] place this number closer to $200 billion. The Federal Bureau of Investigation (FBI) has estimated fraudulent billings to health care programs, both public and private, at between 3 percent and 10 percent of total health care expenditures.[5]

In 2010 alone, Medicare and Medicaid paid an estimated $68.3 billion in improper payments.[6] In 2008, it was reported[7] that Medicare spent less than two tenths of a cent of every dollar of its $456 billion annual budget combating fraud, waste and abuse.[8] Adding further injury is the increased incidence of identity theft. More than 1.5 million people have been victimized by medical identity theft, at an average cost of $20,000 to the victim.[9]

These statistics represent avoidable health care costs that directly impact the cost and quality of health care for every American. Health care fraud and abuse not only contribute to higher insurance premiums, but also every dollar spent on fraudulent or abusive claims reduces the amount of money available to improve the quality of care for those incurring legitimate expenses.

The National Health Care Anti-fraud Association (NHCAA) conservatively estimates that 3 percent of all health care spending, or $60 billion, is lost to health care fraud.

---

[1] <https://www.cms.gov/NationalHealthExpendData/downloads/NHEProjections2009to2019.pdf>.

[2] <http://www.cnsnews.com/news/article/medicareand-medicaid-made-70-billion-im>.

[3] National Health Care Anti-fraud Association, "Consumer Alert: The Impact of Health Care Fraud on You!" <www.nhcaa.org> (Oct. 1, 2009).

[4] October 2009 Thomson Reuters Report, <http://www.reuters.com/article/2009/10/26/us-usa-healthcare-waste-idUSTRE59P0L320091026>.

[5] Federal Bureau of Investigation, "Financial Crimes Report to the Public, Fiscal Year 2007," (May 2008).

[6] Kathleen M. King Director, Health Care, Government Accountability Office. Written Testimony Before the Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, Committee on Homeland Security and Governmental Affairs, U.S. Senate, March 9, 2011, <http://www.gao.gov/new.items/d11409t.pdf>.

[7] Miami Herald, August 11, 2008.

[8] Ibid.

[9] Ponemon Institute, 2011.

To date, success in stemming health care fraud, waste and abuse across commercial and government programs has been far less than satisfactory. As the costs associated with health care coverage reach unsustainable levels, traditional approaches to combating fraud, waste and abuse become increasingly inadequate. Today most fraud detection and recovery is done at the back end of the workflow. Claims are submitted by providers and are paid without a thorough review to determine their legitimacy. If, after a claim has been paid, the payer finds it questionable, it must then embark on the laborious, costly and resource-intensive process of trying to recover the money that has already gone out the door. The results are, at best, partially successful, and often less than that.

It is clear that the industry must migrate to a fraud control model that integrates fraud prevention and detection at the front end of the payer workflow, applies analytic controls throughout the workflow, and incorporates post-pay detection and recovery processes at the back end of the work flow. Claims review processes that incorporate rulesbased data analytics, predictive modeling and linking technologies allow commercial and government payers to identify fraud before an ineligible claim is paid. However, state and federal prompt pay laws and recently enacted Medical Loss Ratio (MLR) regulations affect the ability of payers to successfully implement pre-paid fraud control.

This white paper will examine the pre- and post-payment paradigms currently at work in the U.S. health care system and will delve into why adopting pre-payment fraud controls is critical to reducing fraud, waste and abuse and maintaining a financially sustainable U.S. health care system.

Current regulations drive outdated paradigm

Prompt pay laws reflect the current paradigm that puts quick payment of provider claims above all other priorities in the payment workflow. They set standards for the prompt settlement of health care claims and are a key component of the health care payment paradigm. The laws, which are both federal- and state-specific, require health maintenance organizations (HMOs) and health insurance companies to pay claims within 15 to 45 days of receipt, depending on the specific statute or regulation, except in cases where the obligation to make payment is not reasonably clear or additional information is required to process the claim.
Health plans that fail to pay within the allotted time period are required to pay interest on the final amount paid to the provider. Additionally, Section 1876g(6)(A) of the Social Security Act requires prompt payment of claims submitted under Medicare risk-sharing contracts. The Secretary of the Department of Health and Human Services (HHS) is authorized to enforce this requirement, and is empowered to fine HMOs that are non-compliant. Federal law requires that 90 percent of clean claims be paid within 30 days and that 99 percent be paid within 90 days.

Claims review processes that incorporate rules-based data analytics, predictive modeling, and linking technologies allow commercial and government payers to identify fraud before an ineligible claim is paid.

Payers who fail to meet these thresholds are subject to interest penalties applied in the same manner as those outlined above for private payers. The high volume of claims that Medicare processes—an estimated 4.4 million claims per day—has no bearing on the required payment timelines.

Given the large volume of claims in both the commercial and government segments, only a small fraction of suspicious claims are reviewed at all, even retrospectively. If fraud is proven, the government and commercial health plans are left to try to recover money that has already been paid out. A hard look at the current paradigm quickly reveals that reviewing or auditing only a small portion of claims and retrospectively attempting to recover the payment of fraudulent claims is not an effective approach to reducing health care fraud and abuse.

Health care reform

Health care reform has cast a bright light on the issue of fraud, waste and abuse and it is changing the way we do business. It is unclear what the final version of this iteration of health care reform will look like when the dust settles, but what is known is that money paid for fraudulent or abusive claims is money not spent on the delivery of quality care. This is simply not acceptable. Through the ACA and other reforms, HHS, the Centers for Medicare and Medicaid Services (CMS) and the FBI are aggressively transforming their approach to combat fraud, waste and abuse in the health care industry. It is incumbent upon health insurance executives to understand the risks facing their organizations and to be prepared for the tidal wave of increased enforcement, enhanced financial penalties and more stringent sentencing guidelines.

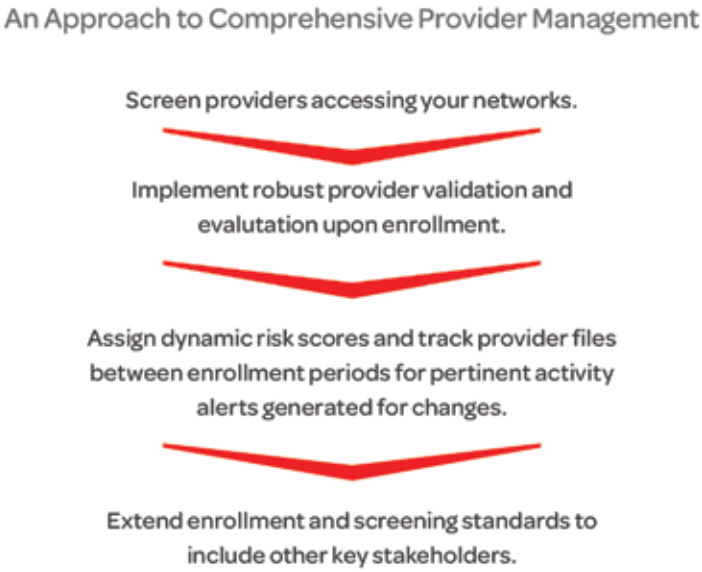
Provider enrollment and screening: As required by the ACA, the CMS recently published the final rule (CMS 6028-FC) on new provider enrollment and screening standards for Medicare, Medicaid and the Children's Health Insurance Program (CHIP). These provisions must be in place by March 25, 2011, for all new provider applicants and by March 23, 2012, for all currently enrolled providers. The enhanced provider enrollment rules are designed to ensure that providers and suppliers are screened according to the perceived risk of fraud, waste and abuse associated with their provider type before being allowed to enroll in these federal programs. The new health care rules also encourage adoption of new strategies to tackle fraud using provider risk scoring and predictive modeling techniques.

Through the ACA and other reforms, HHS, the CMS and the FBI are aggressively transforming their approach to combat fraud, waste and abuse in the health care industry.

Provider risk scoring models can identify problem providers that would not have been identified by other screening methods. LexisNexis® analytics considers thousands of attributes to identify data patterns that can be used as indications about the level of risk associated with a particular provider. LexisNexis takes things a step further by applying its unique data linking technology. In addition to considering whether a provider had any sanctions levied against him, the LexisNexis fraud prevention solutions search billions of public records to help determine if the provider is currently or has ever been the subject of any criminal conviction, including those involving non-health care-related activities, or if the provider has recently engaged in any legal action, such as bankruptcy or repossession of personal property. The information searched includes over 34 billion proprietary and non-proprietary public records. Many of these records are used to calculate risk scores based on years of experience understanding the significant implications of seemingly subtle changes in attributes like addresses. LexisNexis leverages its analytics and advanced linking technology to then filter and link that information, based on relevance, to an entity, individual or business. Records are linked by matching not just one element of relevant information, but as many as 14 different elements. This core proprietary technology is used to ensure the integrity and accuracy of information contained not only in our customers' data but across multiple databases, producing a more secure fraud solution that quickly identifies and connects relevant information and correlates relationships between entities that would otherwise go unnoticed. This dynamic technology evolves as an entity, business or individual's history evolves, constantly taking into account new information, providing the most recent and relevant relationship information to our customers.

Once data patterns and relationship links are found, the LexisNexis provider risk scoring model uses that information to develop predictions about the level of risk for fraudulent or abusive billing associated with providers who meet certain profiles. Health plans that incorporate this type of predictive modeling risk scoring into their provider enrollment processes can establish additional criteria for reviewing claims submitted by high-risk providers before those claims are paid. This reduces the likelihood that dollars will be spent on fraudulent or abusive claims.

LexisNexis leverages its analytics and advanced linking technology to then filter and link that information, based on relevance, to an entity, individual or business.



Program integrity begins with knowing your providers.

In addition to its enhanced provider screening and enrollment requirements, the ACA addresses fraud through payment processes as well. Under the ACA, federal health care programs may:

1. Suspend payments to a provider or supplier when a credible allegation of fraud exists;

2. Place a temporary moratorium on enrollment for those categories of providers demonstrating a high risk for fraudulent or abusive claims practices. Payers will be on the lookout for trends that may indicate health care fraud, including using advanced predictive modeling software, such as that used to detect credit card fraud. The program can temporarily stop enrollment for a category of high-risk providers; and

3. Terminate providers from state Medicaid programs when they have been previously terminated by Medicare or another state Medicaid program, and also authorize the CMS to terminate providers and suppliers from Medicare when they have been separately terminated by a state Medicaid program.

To make these new rules even more effective, private insurers, the CMS and the FBI should work together to reconcile screening processes. Private insurance companies should be encouraged, and certainly managed care payers will be encouraged, to adopt methods and assessment tools to uncover unusual patterns of provider activity. Investments in fraud prevention and detection solutions would help discourage and detect fraudulent activities up front and avoid the loss of billions of dollars paid for ineligible claims.

Medical Loss Ratio: The Medical Loss Ratio (MLR) is the total amount a health insurer pays out in claims costs and adjustment expenses divided by the total earned premium. The ACA requires commercial health insurers to spend a minimum of 80 percent of premium dollars earned in the individual and small group markets on claims and adjustment expenses; 85 percent of premium dollars earned in the large group market must be spent on claims and adjustment expenses. It is important to note that these are minimum ratios; the ACA gives states the authority to enact even stricter MLR requirements that would supersede the federal requirements. At least one state has enacted stricter requirements: Massachusetts imposes a 90 percent MLR requirement. Payers who fail to meet the stricter of the two requirements—state or federal—will be required to return the difference between their actual MLR and that required by law to their members in the form of a rebate.

Measurement of MLRs will begin in 2011, with the first of any applicable rebates scheduled for delivery to customers in 2012. These requirements do not currently apply to limited benefit plans that offer only basic benefits, such as a prescription drug discount card, and coverage for doctors' visits and lab tests (also known as mini-med plans); however, companies that provide these plans are required to collect data so that federal regulators can determine if and how to apply MLRs to them in the future.

In November 2010, HHS issued final rules outlining those expenses that can and cannot be included in the calculation of a payer's MLR. Any expense not included in the MLR must be paid for out of the 15 to 20 percent of "discretionary" income that remains after MLR-eligible expenses have been paid. This includes the day-to-day expenses of keeping the lights on and the telephones operating; the cost of salaries and employee benefits; and implementation of regulatory mandates such as HIPAA 5010, the move from ICD-9 billing codes to ICD-10 billing codes and technological changes required for compliance with the new administrative simplification provisions of the ACA. Unfortunately, while the MLR rules do allow plans to receive credit for any dollars recovered through fraud, waste and abuse investigations, it is still very much an open question as to whether they allow credit for any dollars spent on prepay fraud activities or money spent on post-pay fraud, waste and abuse activities that do not result in financial recovery.

The Medical Loss Ratio (MLR) is the total amount a health insurer pays out in claims costs and adjustment expenses divided by the total earned premium.

Increased criminal sanctions: Despite these challenges, the potential cost savings associated with prepay fraud, waste and abuse activities combined with expansion of the False Claims Act and changes to the Stark Law and Anti-Kickback Statute by federal health care reform create a compelling argument for private payers to invest in pre-payment programs.

C-suite exposure: The ACA significantly relaxes the standard of criminal culpability in the federal courts as it relates to health care fraud. Prior to the ACA, the government had to prove that a defendant had "knowingly and willfully" executed or attempted to execute a health care fraud scheme. The Act amended the general criminal Health Care Fraud Statute (18 U.S.C. §1347) by inserting language stating that it is no longer necessary for a person to have knowledge of or specific intent to violate the Anti-Kickback Statute to be guilty of health care fraud. As a result there is no longer a requirement for the government to prove criminal intent to gain a conviction. A health plan executive or board member whose organization is accused of committing health care fraud is no longer shielded by pleading lack of knowledge. The "I didn't know" defense is gone.

The ACA also significantly expands the definition of what can be considered an original source of incriminating information and narrows the scope of what is considered public disclosure, making it considerably easier to build a case for prosecution of health care fraud.

Finally, the new law expands civil monetary penalties for health care fraud, requires the Federal Sentencing Guidelines to be amended to increase sentences for defendants convicted of federal health care offenses and adds violations of the Anti-Kickback Statute to this category of offense. Effective November 2011, Federal Sentencing Guidelines will be amended to provide:

- A two-level increase in the offense level for any defendant convicted of a federal health care offense related to a government health care program that involves a loss of between $1 million and $7 million;
- A three-level increase for losses of $7 million to $20 million; and
- A four-level increase for losses of more than $20 million.[10]

[10] Sale, Jon A., Esq. and Benson Weintraub, Esq. P.A. "Emerging Trends in Criminal Health care Law Enforcement: The Patient Protection and Affordable Care Act of 2010 Reduces the Criminal Mens Rea Requirements for Health care Fraud and Increases Penalties Under the federal Sentencing Guidelines," The Health Lawyer, Volume 23, Number 3, February 2011.

A health plan executive or board member whose organization is accused of committing health care fraud is no longer shielded by pleading lack of knowledge. The "I didn't know" defense is gone.

According to a report released by America's Health Insurance Plans (AHIP),[11] private payers estimate anti-fraud programs can save their members as much as $300 million per year owing to savings in operational costs. Stricter laws, meaningful penalties and the opportunity for substantial cost savings make investment in advanced analytics designed to incrementally ratchet down risk within the workflow a smart business decision for private payers.

And they aren't the only ones getting in on the act. The ACA greatly enhances the authority of the Secretary of HHS to strengthen provider enrollment standards, promote compliance with program requirements, enhance program oversight (including requiring greater reporting and transparency) and strengthen the government's response to health care fraud and abuse.

Market forces driving new paradigm: Prepayment fraud detection and social network analytics

In May 2009, the Department of Justice (DOJ) and HHS announced the creation of the Health Care Fraud Prevention and Enforcement Action Team (HEAT). With the creation of the new HEAT team, fighting Medicare fraud became a Cabinet-level priority for both the DOJ and HHS. Last year, the federal task force arrested 931 people in illegal billing schemes worth more than $2.3 billion, a 23 percent increase over the previous year. In 2010, it also recovered a record-breaking $4 billion through noncriminal penalties levied on Medicare and Medicaid providers who made improper claims to federal and state agencies. As impressive as these numbers are, the recovered amount is a small percentage of the total amount of improper payments made by Medicare last year. In a March 2011 report issued by the Government Accountability Office (GAO) for the House Energy and Commerce Oversight Committee hearing on Medicare and Medicaid fraud, the GAO estimated that the CMS could save as much as 25 percent of the amount being spent on certain services by refining payment methods and encouraging efficient provision of services. Recommendations for achieving these cost savings include implementation of an effective physician profiling system, such as that now required under the provider enrollment and screening provisions of the ACA. During the hearing, CMS Program Integrity Director Peter Budetti testified that it is the goal of the CMS to move away from the traditional pay-and-chase model of fighting health care fraud to a more proactive model that will prevent fraud from occurring in the first place. Experts testified that such an approach could net Medicare as much as $70 billion[12] per year in savings.

According to a report recently released by AHIP, private payers estimate anti-fraud programs can save their members as much as $300 million per year owing to savings in operational costs.

[11] <http://www.ahipresearch.org/PDFs/22_FRAUDREPORT.pdf>.

[12] <http://www.thefiscaltimes.com/Articles/2011/03/10/Medicare-Fraud-A-70-Billion-Taxpayer-RIpoff.aspx>.

To fuel additional enforcement initiatives, the ACA will increase funding to the DOJ and HHS by $350 million over the next five years. Measurable gains in health care fraud prevention hinge on the ability of both government and private payers to integrate fraud risk controls at the front end of their claims payment workflow processes. Effective fraud detection is best achieved through a layered approach to claims analysis, including identity analytics, claims analytics (predictive modeling and rules-based fraud detection) and social network analytics.

Identity analytics: An important consideration in the development of new approaches to reducing fraud is recognizing the implications of health care fraud on patient safety. The silos that commonly exist between a health insurer's payment operations and post-payment fraud investigation are dangerous. According to the FBI, one of the most significant trends observed in recent health care fraud cases is the willingness of medical professionals to risk patient harm in their schemes. FBI investigations into several offices are focusing on subjects who conduct unnecessary surgeries, prescribe dangerous drugs without medical necessity, and engage in abusive or sub-standard care practices.[13]

Implementation of fraud risk and identity management programs that reflect more advanced fraud prevention models in health care as well as learning from best practices in other industries are needed to help prevent this kind of hazardous and costly fraud. Recent advances in health IT enable realistic implementation of these models. Addressing fraud risk via the current pay-and-chase model is not a sufficient approach. Financial pressures, reform and increased enforcement require a fundamental shift, which is now possible. Implementation of identity verification, authentication and screening mechanisms at the beginning of the payment workflow is critical to this change.

With a "true" enterprise-wide approach to identity management to verify and authenticate the identity of providers and evaluate their backgrounds, a health plan's current provider file can be evaluated for derogatory information or indications of risk; new providers who are accessing the system for the first time can do so in a fast, efficient and user-friendly manner; providers will have their identity verified and be evaluated for enrollment; and providers' identities can be periodically reviewed for critical changes between enrollment periods. This will lead not only to recovering monies post-payment, but also to removing some providers from a payer's network altogether or severely limiting the scope of services for which they are paid (in pre-pay mode).

The silos that commonly exist between a health insurer's payment operations and postpayment fraud investigation are dangerous.

[13] Federal Bureau of Investigation, Financial Crimes Report to the Public, Fiscal Year 2007.

For example, LexisNexis offers a comprehensive identity management program that allows users to:

1. Verify the identity of an individual (Do you exist?);

2. Authenticate that identity (Are you who you say you are?);

3. Provide information necessary to evaluate the identity's eligibility for participation (so the user can assess against legislation, regulations and rules to determine if a provider meets eligibility criteria); and

4. Provide ongoing monitoring of the individual so the user can ensure that s/he continues to meet eligibility criteria.

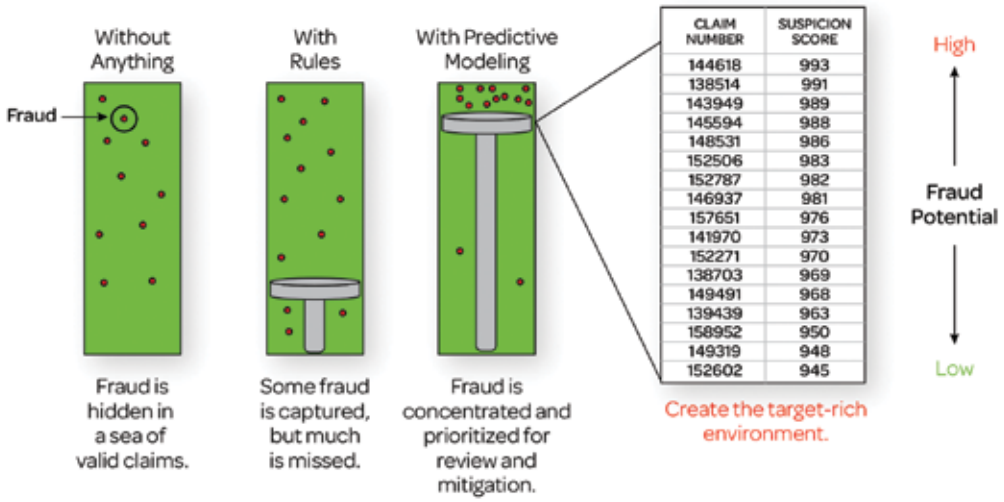
LexisNexis will notify its users when an individual or entity exhibits high-risk behavior that may signal a change in eligibility.

Claims analytics: Comprehensive pre-pay claims analytics consist of rules-based screens and edits as well as predictive modeling that identifies the potential for improper payments by "scoring" claims and/or providers before a claim is paid.

Traditional rules-based fraud detection systems that analyze claims and identify outliers are most frequently deployed post-payment. Moving this operation to the front end of the claims payment process and complementing it with predictive modeling techniques is key to changing the game in favor of providers that are giving proper care and payers who are attempting to pay legitimate claims as quickly and efficiently as possible. In an environment that employs pre-pay analytics, payers can analyze historical claims data to identify fraudulent and abusive patterns and trends. This information can then be used to identify characteristics of a claim or provider billing habits that could suggest fraudulent activity. Next, that information is applied to claims as they are being processed—before they are paid—to separate out those that may require further review. Combining rules-based analytics with predictive modeling techniques is a far more effective way to detect sophisticated fraud schemes than relying on rules-based analytics alone. Whereas a rules-based approach allows the payer to identify those characteristics they know suggest suspicious behavior, predictive modeling applies algorithms that identify abnormalities not immediately apparent. Predictive modeling employs advanced methods to detect fraudulentb patterns across claims by considering multiple factors that are too subtle and complex for traditional rules-based applications to identify. The value of predictive modeling is further enhanced by its "live" nature. Predictive models "learn" through experience; each time the model is run, more data is accumulated and analyzed. The model also collects and applies results from prior investigations and audits. The more information the model collects, the better it is able to recognize patterns similar to those previously determined to be fraudulent or abusive, allowing the model to adjust to the changing behavior of providers.

Combining rules-based analytics with predictive modeling techniques is a far more effective way to detect sophisticated fraud schemes than relying on rules-based analytics alone.

The Value of Predictive Analytics



Predictive analytics provide a score for each claim, policy, etc., allowing activity to be concentrated on areas that have the highest probability of financial return

The idea of applying predictive modeling to the claims payment process is not new; however, until recently, its promise has remained largely unfulfilled. Early adopters incorrectly assumed that one need only apply the same approach to predictive modeling that had been used so successfully in the credit card industry. It soon became clear that the complexity, variability and inaccuracy of data found in health care claims made that impossible, generating far too many false positive results to make the analysis useful. A false positive is a claim flagged as problematic that turns out to be legitimate after a time-consuming manual review. Pulling these claims out of the payment workflow, only to find they are payable, causes significant problems—not the least of which are the penalties associated with late payment of a legitimate claim. Equally important to payers is the loss of time, resources and money spent unnecessarily investigating a false positive, and the damage done to relationships with providers who feel they have had their integrity wrongly questioned and may have suffered financial harm as a result of the delay in payment.

There are two ways to address these issues. In much the same way that the inevitability of pre-pay fraud detection has been talked about for years—almost daily since the health care reform debate began—predictive analytics must be used to review every claim before it is paid.

First, we must explore various statistical models to determine which ones will keep false positives to an acceptable minimum. As more companies enter this market with experience from other industries, particularly those that involve modeling of medical claims in other contexts, more and more varied models will be tried on health care data, and we will begin to move toward predictive models that satisfy the requirements for low false positives that will allow inclusion at the front end of the payment workflow. A key decision in the predictive modeling process is setting the "cutoff" score for flagging the claim. The higher the score, the higher the probability that the claim is suspicious. A very high cutoff score means that fewer claims will be flagged, but the accuracy of those flagged will be very high and there will be fewer "false positive" errors.

LexisNexis has been able to leverage its experience with health care claims processed by the property and casualty industry to develop provider or claim with minimal danger of generating a false positive result.

Second, we should take a layered approach to what can be described as "automated triage."

Resources will always be an issue in pre-payment fraud control. When a claim is flagged, unless it violates an absolute rule, the most expensive resource of all—a skilled person—needs to look at that claim and make a judgment about it. By taking a layered approach to pre-payment fraud control, the claims that reach that skilled person's desk can be refined so that the claims they receive are in fact those most likely to represent fraudulent or abusive activity. Skilled individuals will deal less and less with "noise" and more and more with "signal."

There are those who worry that the pre-payment approach outlined here will result in unmanageable amounts of data being generated for action by already over-burdened personnel. In order to avoid needing additional personnel and further straining already limited budgets, it is critical to ensure that the quality of data provided by the predictive model is clear and actionable. However, with effective fraud control, the ROI may offer justification for additional personnel.

Social network analytics: Health care insurers increasingly face escalating sophistication of fraudulent behavior by networks of participants, including crime rings. The NHCAA has noted that, in recent years, law enforcement agencies and health insurers have witnessed the migration of some criminals out of drug trafficking and other lines of crime into the safer and more lucrative business of perpetrating collusive fraud schemes against Medicare, Medicaid and private health insurance companies. Much of the fraud, waste and abuse that plague health care payers is the result of organized, collusive activities among providers and between providers and patients. The identification of large-scale fraud rings is important and creates headlines to raise awareness of the problem. More localized collusion can be harder to find and is much more prevalent. Social network analysis (SNA) can help identify relationships, links and hidden patterns of information sharing and interactions within potentially fraudulent clusters, including:

- Patient relationships with known perpetrators of health care fraud;
- Links between recipients, businesses, assets, and relatives and associates;
- Links between licensed and non-licensed providers; and
- Inappropriate relationships between patients, providers, employees, suppliers and partners.

A key decision in the predictive modeling process is setting the "cutoff" score for flagging the claim. The higher the score, the higher the probability that the claim is suspicious.

SNA provides a rich set of metrics. Its adoption is being driven by the availability of more sources of information (including public records and the social web), and by the fact that network-analysis software is becoming more robust and user-friendly. Vice President Joe Biden indicated that such software would be leveraged to combat fraud within the government's Medicaid and Medicare health care schemes.[14]

Typical SNA outputs include visualization of relationships and the degree of correlation and confidence associated with the linkages between relationships.

Traditionally insurers have attempted to identify collusive relationships through phone and address information that the insurer may have for the suspected individuals or entities, combined with a limited amount of public information intended to strengthen the connections found through phone and address records, or identify potential additional links. Insurers then use a "visualization tool" to eliminate weak or less important links. Business rules or queries are applied to filter the visualization starting points.

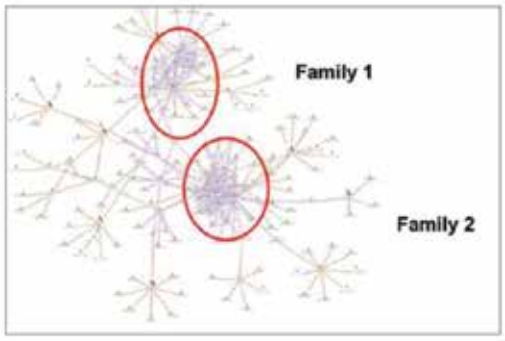
Unfortunately, because the relationship characteristics used in this approach are subject to frequent change (phone and address) and the amount and types of information used to validate the suspected relationships is so limited, this approach often leads to an unacceptable number of false positive results. The limited scope of data considered also results in many missed opportunities to identify additional relationships or links, which means that we are much more likely to be addressing symptoms of a problem rather than getting to its root. Finally, the traditional approach is extremely labor-intensive and its success is highly dependent on the expertise of the individual conducting the analysis.

Social network analysis (SNA) can help identify relationships, links and hidden patterns of information sharing and interactions within potentially fraudulent clusters.

14 "Mining Social Networks: Untangling the Social Web", The Economist, September 2, 2010.

Today, Today, advanced technology highly optimized for systemically determining relationships and links is used to "automate" much of the work, and access to public records data beyond phone and address information creates links between entities that are more accurate and much more stable over time. LexisNexis uses its extensive public records database, High Performance Computing Cluster (HPCC) and advanced data analytics to identify collusive relationships. Along with identifying providers of interest, this tool allows payers to address fraud, waste and abuse much more broadly than the traditional bill-level approach.

Using its own internal data and linking technology, a private insurance carrier found just one link between seven collusive insurance fraud schemes representing hundreds of suspect claims.



By using LexisNexis advanced linking technology and linking the carrier's own internal data to the LexisNexis public records database, LexisNexis was able to identify 11 additional potentially fraudulent schemes (representing hundreds of already paid claims) directly related to the original seven. In addition, LexisNexis identified two families that appeared to be at the center of the fraudulent scheme.

Conclusion

The U.S. health care system is in a state of flux. Daily reports of appeals regarding the constitutionality of the health care reform statute as well as attacks on specific pieces of the bill mean that both government and commercial payers and providers are making hard decisions about where to spend their resources. The one thing that everyone can agree on is that every penny spent on improper payments, care that never took place and dangerous manipulation of patient care to increase billings directly prevents us from achieving the goal of lowering costs and increasing quality of care. In its 2009 report, "The Long-Term Budget Outlook," the Congressional Budget Office (CBO) projected that without significant changes in policy, total spending for health care will be 31 percent of GDP by 2035 and increase to 46 percent by 2080.[15] This trend must be reversed as quickly as possible, and prevention of improper payments is foundational to this effort. The best possible way to treat certain chronic diseases may be debatable, but the need to stop fraudulent and wasteful payments is not. By combining identity and entity resolution, rules-based claim and clinical review, complex linking analysis and predictive analytics into a seamless workflow, we will come closer to migrating an integrated pre-pay fraud solution to a real risk control environment. This migration from a post-pay fraud control workflow to a pre-pay fraud control workflow has the potential to eliminate billions of dollars in improper payments due to fraud, waste and abuse. This is not just a health care imperative, but also a national economic imperative that must be addressed immediately. The analytics exist. It is time for those analytics to be implemented and the hard choices that enable that implementation to be made to ensure that we remain at the forefront of quality care for all Americans.

[15] Source: http://www.cbo.gov/ftpdocs/102xx/doc10297/Chapter2.5.1.shtml

Additional Sources

- "Moving Forward with Reform: The Health Plan Agenda for 2011 and Beyond," Business Wire, March 16, 2011.
- <http://www.healthcare.gov/news/factsheets/medical_loss_ratio.html>.
- <http://www.ahipresearch.org/pdfs/FraudPrevention2011.pdf>.
- <http://www.thefiscaltimes.com/Articles/2011/03/10/Medicare-Fraud-A-70-Billion-Taxpayer-Ripoff.aspx>.
- "Medical Loss Ratio to Affect Entire U.S. Health care Sector," Gartner, August 24, 2010.
- "U.S. Health care Reform Advances Fraud Prevention," Gartner, December 3, 2010 <http://healthreform.kff.org/>.

For More Information:

Call 800.869.0751 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 assess, predict and manage risk. Combining cutting-edge technology, unique data and advanced analytics, LexisNexis Risk Solutions provides 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 world leading provider of professional information solutions.

Our identity management solutions assist states with ensuring appropriate access to public benefits, enhance program integrity and operational efficiency, reduce the impact of identity theft and fraud, and proactively combat fraud, waste and abuse throughout government programs. Our health care solutions assist payers, providers, and integrators 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. The NAC is in the unique position to benefit by overlaying state data with the complex analytics of LexisNexis's solutions.

LexisNexis® | Health Care