Moving Beyond ‘Pay and Chase’ to Fight Healthcare Fraud

Healthcare providers that embrace predictive analytics can prevent the payment of false claims before they undermine business performance.

Executive Summary

Financial losses in the U.S. due to healthcare fraud are estimated to range from $75 billion to a staggering $250 billion a year, accounting for as much as 10% of U.S. health expenditures. Experience shows that preventing fraudulent payments is far more cost-effective than post-payment recovery efforts.

This white paper explains why it is imperative to move beyond the historic “pay and chase” model, to a data-driven methodology that utilizes analytics to perform targeted, clinically-relevant fraud identification and prevention. It then describes how such data analysis can be used to detect and help prevent common types of fraud.

Fraud Flourishes Amid Volume, Complexity

The sheer volume and complexity of the $2.6 trillion U.S. healthcare system makes combating fraud a daunting challenge. Every year, hundreds of thousands of service and product providers file billions of claims. Medicare alone pays 4.4 million claims a day to 1.5 million providers across the country. Beyond the sheer number of claims to monitor, healthcare insurance payers are outgunned by fraudsters, many of whom have the specialized knowledge on which to base false claims, such as best clinical practices, medical terminology and specialized codes.

The lack of a single claims repository also makes it more difficult to detect multiple claims for the same product or service. Fraud detection is yet more complex because most providers bill multiple private and public payers, with each payer having visibility only into the claims it receives and adjudicates.

Examples of provider-perpetuated waste, fraud and/or abuse include:

- Billing for unnecessary medical services, equipment or prescription drugs.
- Billing for services that were not actually provided.
- Up-coding, or inappropriate use of current procedural terminology (CPT) and diagnosis-related groups (DRG) codes to gain higher reimbursement.
- Submitting claims for non-covered persons.
- Scheduling more frequent visits than required to increase reimbursements.
- Billing for services for which the provider is not qualified.
- Duplicate billing for services rendered.
- Payments stemming from kickbacks.
- Keeping overpayments made in error by payers.
Today’s retrospective approaches do not identify fraud or efficiently prioritize investigative efforts on a timely basis. A shortage of investigative technology, money and staff leads to reactive and fragmented fraud management processes. Recovering fraudulent payments after the fact is not only more difficult than prevention, but it also requires large amounts of money and staff time.

Meanwhile, member-perpetrated fraud, waste and abuse are also proliferating. Examples include:

- Falsifying or modifying prescriptions to obtain alternative substances or medications, or more medications than prescribed by the physician.
- Members sharing plan membership ID cards with non-members.
- Members failing to disclose supplementary health insurance coverage.
- Members obtaining unnecessary equipment and supplies.

The Analytics Answer

Many observers, including the American Medical Association, have long suggested that the most efficient way to combat healthcare fraud is through targeted, streamlined analytics. The reactive “pay and chase” model should be replaced by a multi-pronged approach that uses analytics to enable targeted, clinically-informed fraud identification and prevention.

Such a system would streamline and integrate commercial, federal and state-level anti-fraud programs and audits to improve coordination and detection rates. It would build multidimensional predictive models to detect fraud at a very early stage, and develop innovative solutions to reduce costs by minimizing the administrative burden and more efficiently targeting enforcement.

A successful fraud detection system would also stay up to date with continuously evolving fraud and abuse schemes, detect suspicious claims with a high degree of accuracy before they are paid and offer a cost-effective approach to triaging large volumes of claims.

By proactively utilizing analytics, such a system could identify aberrant claims in real time and cross-reference them with claims from other data sets to flag potentially fraudulent activity. Doing so requires the use of dynamic, configurable predictive modeling tools that support the following:

- Close to real-time pre-payment detection.
- Recognition of non-linear patterns, such as clustering, discriminant analysis and decision tree.
- Linear pattern identification, such as trending and heuristics to “learn” more about which claims patterns are the most suspicious.

Using analytics also requires healthcare fraud models that are designed and tested to identify fraud, waste and abuse indicators, such as:

- Unusual geographic concentration/dispersion of participants.
- High-frequency utilization designs.
- Uncharacteristic practice patterns.

Such advanced predictive analytics can recognize potential fraud patterns that are undetectable using conventional methods, delivering actionable results through automated detection (see Figure 1, next page). These approaches include:

- **Stratifying numbers** to identify unusual (i.e., excessively high or low) entries.
- **Statistical parameters**, such as averages and standard deviations to identify outliers that could indicate fraudulent activity.
- **Trend charts to identify patterns** of potential fraud among data elements.
- **Digital analysis** to identify unexpected occurrences of digits in naturally occurring data sets.
- **Bridging diverse sources** in the healthcare ecosystem to identify the occurrence of identical values (such as names, addresses and account numbers) that should not exist.
- **Identical value identification** to flag duplicate transactions, such as payments, claims or items in expense reports.
- **Link analysis**, which establishes relationships among claims, people and transactions by discovering related claims in seemingly unrelated instances.
- **Comparing summed and totaled charges using control charts** to identify outliers and ambiguous claims.
- **Validating entry dates** to identify suspicious or inappropriate times for postings or data entry.
Key Requirements

Analytics systems that detect and prevent healthcare fraud should offer the following features and capabilities:

- **Dynamic rules engines** as the system foundation, testing each transaction against a predefined set of business rules to detect known types of fraud or abuse and flag suspicious claims.

- **Anomaly detection algorithms**, based on KPIs for specific tasks or events, baselined with thresholds that alert for potential fraud. Outliers or anomalies should also be identified to indicate new or previously unknown patterns of fraud.

- **Predictive modeling that** utilizes data mining tools to build models that produce fraud propensity scores. Such modeling uses statistical analysis to discover previously unknown fraud schemes based on previously unidentified metrics.

- **Social network analysis and multi-entity fraud detection**, using social tools and techniques to identify organized fraud activities by modeling relationships between entities in claims. These entities may include locations, service providers, members, addresses or telephone numbers. These tools can be tuned to display link frequencies that exceed a programmed threshold.

Case Examples

Typical areas where data analysis applications can detect and prevent healthcare include:

- Highlighting billing for medically unnecessary tests.
- Identifying false/invalid/duplicate entries.
- Highlighting excessive use of DRGs that have historically posed a high risk for fraud.
- Identifying excessive billing by a single physician.
- Identifying employee overtime abuses.
- Reporting claims against authorization records for new or terminated employees.
- Identifying multiple payroll deposits to the same account.
- Matching the OIG (Office of Inspector General) list of excluded providers with employee master files.
- Finding kickbacks paid in exchange for referring business by detecting either analytical or control symptoms or anomalies.
- Identifying charges posted outside of permissible periods.

Predicting Fraud Before it Strikes

Advanced predictive analytics recognize patterns that would be undetectable using conventional methods, delivering actionable results via automated detection.
• Identifying “up-coding” by flagging statistical outliers.
• Analyzing large invoices that lack purchase orders by amount, provider, vendor, etc.
• Validating lists of enrolled employees by comparing them with lists of people receiving health benefits from insurers.

With new fraudulent billing and claims schemes continuously emerging, fraud prevention must consist of a "virtuous cycle," in which the results of the latest data analysis help to fine-tune the algorithms, rules and models used to detect potential fraud. Such a system relies on ongoing validation and measurement of the latest fraud detection models, drawing on ongoing experience to increase their effectiveness (see Figure 2 and sidebar).

Looking Ahead

Healthcare fraud and abuse puts an enormous financial burden on a system that is already facing unprecedented pressure from consumers and legislators to contain costs. The magnitude of potential fraud and abuse savings is so great that as more payers recognize and adopt state-of-the-art detection capabilities, those with antiquated fraud management practices will be at a significant competitive disadvantage.

To meet these challenges, it’s time for health insurers to devote additional resources to predictive modeling technology and real-time analytics. By applying these techniques to fraud prevention, they can avoid the excessive costs and uncertainty of recovering fraudulent payments after they have been paid. Combining multiple techniques offers the best chance for detecting both opportunistic and professional/organized fraud.

A hybrid approach, which integrates knowledge of existing fraud schemes with powerful predictive analysis techniques, can help contain system-wide healthcare costs, while giving providers and payers a competitive edge.

Quick Take

Analytics in Action: A Leading Healthcare Services Company

• **Challenge:** Identify and create new business rules to prevent claims fraud and abuse.

• **Analytics applied:** Rules and anomaly detection.

• **Services provided:**
  > We established a claims analytics team of medical coders, fraud analytics investigators, data miners and SAS programmers to identify and create new rules to flag fraudulent claims.
  > We also created a prospective fraud investigation team made up of healthcare professionals and medical coders to analyze and investigate possibly fraudulent claims triggered by the rules, as well as the resulting anomaly detection to block fraudulent claims.

• **Results:**
  > Saved $8 million by identifying fraud before it happened.
  > Created 24 new business rules, with annual potential savings of more than $18 million.
Footnote


References


About the Author

Nitin Gangwani is a Senior Associate with Cognizant Analytics. With wide experience applying business consulting and analytics in the life sciences, managed markets and healthcare industries, Nitin has delivered strategic consulting and analytics services in the areas of business analysis, requirements gathering, data warehousing, patient claim analytics, campaign management and solution design. He holds an M.B.A. from the Management Development Institute and a B.E. degree from Netaji Subhas Institute of Technology. Nitin can be reached at Nitin.Gangwani@cognizant.com.

About Cognizant

Cognizant (NASDAQ: CTSH) is a leading provider of information technology, consulting, and business process outsourcing services, dedicated to helping the world's leading companies build stronger businesses. Headquartered in Teaneck, New Jersey (U.S.), Cognizant combines a passion for client satisfaction, technology innovation, deep industry and business process expertise, and a global, collaborative workforce that embodies the future of work. With over 50 delivery centers worldwide and approximately 166,400 employees as of September 30, 2013, Cognizant is a member of the NASDAQ-100, the S&P 500, the Forbes Global 2000, and the Fortune 500 and is ranked among the top performing and fastest growing companies in the world. Visit us online at www.cognizant.com or follow us on Twitter: Cognizant.

© Copyright 2014, Cognizant. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the express written permission from Cognizant. The information contained herein is subject to change without notice. All other trademarks mentioned herein are the property of their respective owners.