

Sponsored by:



PAYERS EMBRACE **BIG DATA**



By Gienna Shaw, Editor-in-Chief, FierceHealthPayer

When you crunch the numbers, the insurance industry's risk of loss to fraud is staggering. Imagine the number of providers filing office visit claims. Assume they see 20 patients daily, 48 weeks a year. Just one level of code inflation can cause an insurer to lose over \$50,000 per practitioner annually.

But number-crunching can also help prevent fraud and improve business processes. The key is to pay attention to past and current data—and then use it to look into the future.

Throughout this eBook you'll find examples of how insurers, including Wellpoint, Aetna, Blue Cross and Blue Shield of Louisiana and more, are using data to drive down costs by preventing fraudulent or unnecessary claims, identifying doctors that provide high-quality, low-cost care, improving business processes and streamlining administrative workflows. You'll also learn about the power of predictive analytics to stop fraud before it starts, avoiding the frustrating and costly game of pay-and-chase later.

No one is saying data can do everything—but it sure can do a lot.

"The claims tell a story. The data tell a story. You just have to decipher it," says Alanna Lavelle, director of investigations at Wellpoint, Inc.

USING DATA TO FIGHT FRAUD

4 techniques to catch criminals and stop losing money
by J.M.K. Antonio

Criminals are looting the healthcare system, and catching them is an imperative for insurers. And the debate about cost cutting required by healthcare reform is spotlighting anti-fraud efforts and the dollars they save. Those efforts often depend on data analysis.

Here are four retrospective analysis techniques—and true tales of how payer organizations are using them to foil fraud.

Technique #1: Review employer data

While payers typically analyze provider and member data to find fraud, it's also valuable to study employer-specific claims history. Companies with rich benefits are tempting targets for fraudsters. And recoveries on behalf of employers can help insurers retain self-funded accounts.

Blue Cross and Blue Shield of Louisiana (BCBSLA) analyzed data for a 200,000-employee group and soon uncovered a problem: A chiropractor's office that was seeing staff at a rate and duration far above specialty norms. On-site review showed patients received repetitive, massage-like services that didn't qualify for payment. BCBSLA assessed an overpayment of several hundred thousand dollars.

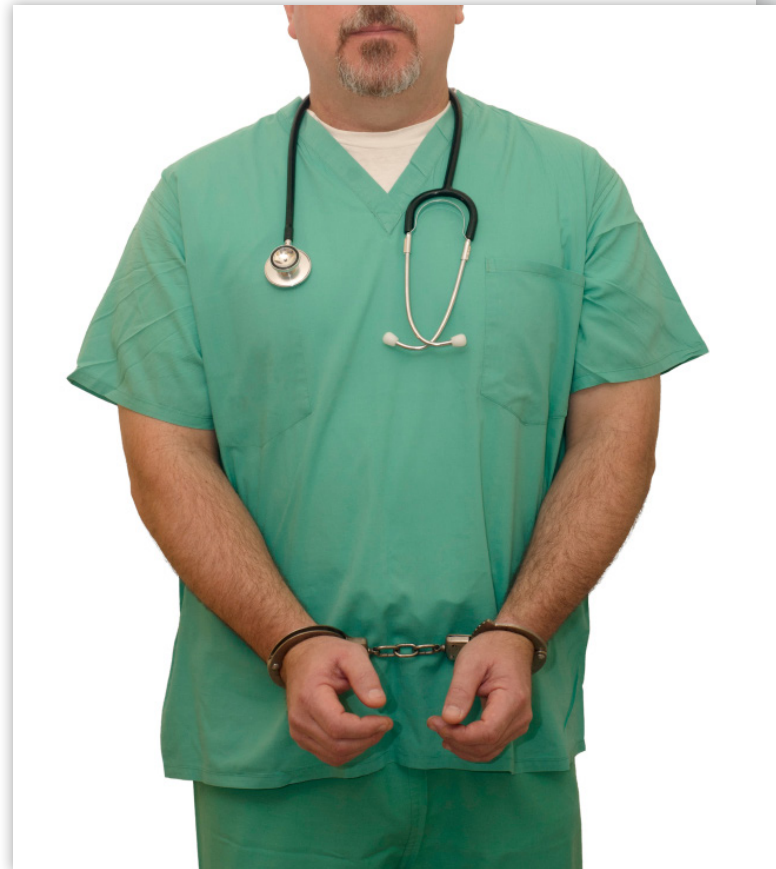


“Watch the money trend and trace it back to why it's trending. Then you'll find the fraud.”

Darrell Langlois, Vice President, Blue Cross and Blue Shield of Louisiana

Wellpoint also found a problem with chiropractic services when it discovered one office that tripled its annual income by servicing patients who worked for the same company. It turned out the chiropractors had set up shop near the group's headquarters and were recruiting patients aggressively: they offered free lunches when people saw them for adjustments and encouraged their families to come on down.

The chiropractors saw some employees three times weekly for non-covered services billed as four units of physical therapy. Once they had member insurance



IDs, the providers filed for services not rendered. They billed 90 physical therapy visits per patient annually, right up to the benefit maximum. These chiropractors were prosecuted and convicted with a court-ordered restitution of \$8 million.

Technique #2: Consider the ubiquitous

“You don't have to look far to see abuse,” says Alanna Lavelle, director of investigations for the southeast and central regions at Wellpoint. “One of the most insidious problems we face involves upcoded office visits.”

Imagine the number of providers filing office visit claims. Assume they see 20 patients daily, 48 weeks a year. Just one level of code inflation can cause an insurer to lose over \$50,000 per practitioner annually. A 2012 report by The Center for Public Integrity said that between 2001 and 2010, Medicare overpaid approximately \$6.6 billion for office visits claimed at the complex level without justification.

Technique #3: Investigate ratios

Darrell Langlois, vice president of compliance, privacy and fraud at BCBSLA, says there are four key ratios to watch with any specialty in any fraud scheme:

- average dollars paid per patient
- average visits per patient
- average dollars paid per medical procedure
- average medical procedures per visit



“If you’re scanning the skies for problems,” Langlois says, “use ratios to follow the dollar trends ... Watch the money trend and trace it back to why it’s trending. Then you’ll find the fraud.”

Lavelle agrees. “The claims tell a story,” she says. “The data tell a story. You just have to decipher it.”

An example: Wellpoint investigators found out-of-network colonoscopy claims with an average reported charge of \$80,000 paid to patients. Many were Georgia poultry workers who visited California for colonoscopies, endoscopies and other procedures.

Providers offered travel incentives including free airfare, hotel accommodations, tickets to Disneyland—even breast implants. Among the patients were Asian immigrants who were persuaded to go west by runners recruited from members’ ethnic groups. Criminal prosecution of the doctors is underway.

Meanwhile, Wellpoint changed its out-of-network payment policy, which underscores an important point: Payers should “close the loop” and use lessons learned in anti-fraud cases to remedy vulnerabilities.

In another scheme uncovered by examining with ratios, BCBSLA identified a general practitioner with a high percentage of office visits compared to his peers. Almost all his patients received high doses of oxycontin for prolonged periods. Patients were complicit in the crime; they received desired drugs without paying for them. The case went into criminal investigation by the FBI and state police. The doctor pled guilty, relinquished his medical license and was sentenced to 17 years in federal prison.



“The claims tell a story. The data tell a story. You just have to decipher it.”

Alanna Lavelle, Director of Investigations,
Wellpoint, Inc.

Technique #4: Analyze codes

According to Langlois, analyzing procedure codes in response to intelligence about problems with them is more useful than unfocused noodling though provider coding patterns.

Case in point: Wellpoint investigated a medical equipment provider’s coding after getting a tip about transcutaneous electrical nerve stimulation (TENS) units. The provider filed for TENS units and then billed again on subsequent dates for each unit’s component parts. Wellpoint paid millions for \$3 nine-volt batteries, lead wires and connections already reimbursed in the unit allowance. Overpayment recovery is underway.

Objective mirrors

Since data are unbiased, they can challenge assumptions about who commits fraud, waste and abuse. It’s easy to believe wrongdoing is committed by organized criminals or fly-by-night equipment suppliers working out of gas stations, but what about the esteemed cardiac surgeon or the trusted oncologist?

“Fraud is present in any level of medical specialty,” Langlois says. By acting on what their data reveal, payers can find opportunities to attack fraud efficiently, even when it rears its head in unexpected places. ●



USING DATA ANALYTICS TO DRIVE DOWN COSTS

Advanced analytics and leveraging massive public records data sets are changing the way health care enterprises detect and prevent fraud. According to the federal website, PaymentAccuracy, the government made nearly \$65 billion in improper health care-related payments, and government agencies have been hard at work trying to put a stop to it—but with limited results. Even though \$1.7 billion was spent to combat fraud, waste and abuse in 2010, less than 10 percent of fraudulent dollars were recovered. Unfortunately, once the money is out the door, it's almost impossible to get back. Criminals have become adept at exploiting this vulnerability—but for the first time, new technologies like data analytics are beginning to tip the scales.

Even though \$1.7 billion was spent to combat fraud, waste and abuse in 2010, less than 10 percent of fraudulent dollars were recovered.

To understand how, let's consider some of the reasons why fraud has become so prevalent:

1. Individuals are getting access to other individuals' identities and using it for fictional medical care making identity theft a growing problem.
2. The Affordable Care Act is introducing a huge amount of new patients into the health care system. Health care entities continue to ask for only a limited range of information to confirm an identity—name, Social Security number (SSN) and date of birth.
2. With the influx of individuals coming into the system, payers will need to take new approaches to cracking down on fraud. Investigative units will benefit from turning to big data and analytics to prevent the wrong people from rendering services and maximizing data by introducing new data sets.

With the influx of new insureds into the system, data analytics and leveraging massive public records must

be added to the enrollment process. Eliminating online applications would make it harder for honest citizens to obtain health care benefits. Current data collection and enrollment systems uses name, social security number, and birth date to run a match against a public records database. If the identity is legitimate, applicants must answer a series of unique questions designed to weed out fraudsters. The quiz is easy to answer for honest citizens but nearly impossible for fraudsters. But what if government agencies asked for information beyond the name, social security number, and date of birth? That's exactly what's being implemented in a series of innovative approaches using big data analytics and identity resolution.

Data analytics can also be used to catch sophisticated crime rings that extract tremendous sums from the vulnerable medical ecosystem. To identify organized crime, agencies are turning to what's being called "social network analytics" to find relationships between people, businesses and assets within massive data sets. It all begins with the data—as much as 50 terabytes of public records.

Here's how it works: a health care agency delivers a list of providers and beneficiaries to its data analytics partner. Using this list alone and an understanding of the agency's mission, the partner cross-checks this information with its public records database to make connections that are otherwise invisible. This process looks across the full spectrum of an agency's data, searching out fraud across the entire provider and beneficiary network and even across multiple jurisdictions or states—uncovering fraud in days or weeks, rather than months.

Today, government agencies are struggling with shrinking budgets and a growing health care need. The White House estimates the sequester alone will cut \$11 billion from Medicare and an additional [\\$1.6 billion](#) from the National Institutes of Health. To drive down costs, agencies must embrace new tools and technologies like data analytics. When matched with good information, intelligent analysis, and a firm understanding of the health care mission, agencies can leverage data analytics to continue to deliver critical services to those in need.



LexisNexis®

6 WAYS TO MINE RETROSPECTIVE DATA*Information ‘discoveries’ that led to business success*

by J.M.K. Antonio

Information is the ultimate business partner. As payers learn to work with it artfully, new meanings develop and organizational intelligence grows. Insurers are using knowledge gleaned from retrospective data analysis to improve efficiency and manage population health.



“We use data to help us understand where to focus our resources to help our provider community and our members.”

Pamela Peele, Ph.D., Chief Analytics Officer,
University of Pittsburgh Medical Center Health Plan

“We use statistical approaches to identify knowledge in data that we may not have known to look for,” says Daryl Wansink, Ph.D., Director of Health Economics at Blue Cross and Blue Shield of North Carolina (BCBSNC). A best practice is letting data reveal what’s happening in business instead of approaching data with prescriptive hypotheses. Along with this receptive stance, experts recommend these tactics:

- hire staff trained to use statistical models in real-world settings or on applied issues; and
- do the preliminary legwork necessary to make data fit for consumption.

“Claims data must be harmonized, standardized and brought up into a groomed layer of information” before payers can use them for purposes beyond reimbursement, says Pamela Peele, Ph.D., chief analytics officer at the University of Pittsburgh Medical Center (UPMC) Health Plan.

Adds Wansink: “Data mining isn’t as productive if you’re dealing with messy or poorly structured data. Reducing noise in your data makes it easier to find signals or trends.”

Here are six discoveries that resulted from these approaches and helped companies fine-tune their business:

1. High-quality, low-cost providers

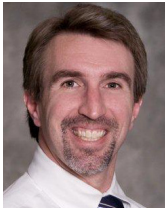
BCBSNC uses data to compare quality and efficiency of care delivered in hospitals and medical practices. BCBSNC shares findings in standardized reports to participating providers. “Doctors are receptive to receiving this type of information because it’s not something they can see from their own administrative data,” Wansink says. “And we’ve been very transparent in providing data to them so they can improve their care delivery.”

For example, not all doctors within a specialty have the same workflow—variations in care may result from inter-specialty referrals. A non-invasive cardiologist, for example, practices differently from a specialist doing only coronary artery bypass grafting.

Data analysis highlights these differences and helps payers refine practitioner comparisons.



In the search for high-quality, low-cost providers, data shows that low hospital reimbursement rates don't always correlate with efficient care. Considering the total cost of care, BCBSNC saw that some facilities with low contracted rates function inefficiently, even though their per-admission cost is less.



“Data mining isn't as productive if you're dealing with messy or poorly structured data. Reducing noise in your data makes it easier to find signals or trends.”

Daryl Wansink, Ph.D., Director of Health Economics, Blue Cross and Blue Shield of North Carolina

Plans can use results of quality and efficiency studies to negotiate rates better and place participating providers correctly in network tiers. Greater patient cost sharing for services by lower-tier providers may drive people to higher quality, lower cost healthcare sources.

2. The 80/20 care coordination rule

“We use data to help us understand where to focus our resources to help our provider community and our members,” Peele says.

An example is UPMC's anti-regression model. It's based on the knowledge that while 80% of members who consume high-cost care in a given year will need fewer services going forward, the remaining 20% will need ongoing management. These 20% are the best focus of care coordination.

In what Peele calls “an iterative process between scientific discovery and discussions with clinical staff,” UPMC flags and engages “intervention sensitive” individuals.

3. Signs of unplanned care

Free text mining in electronic medical records helped UPMC find 60 keywords that identify members likely to receive frequent unplanned care outside relationships with primary care physicians. These signals trigger care management interventions.

4. Program effectiveness evaluation

BCBSNC uses biometric data to measure wellness program effectiveness for stratified participant groups

and tweak the programs in later iterations. Similar retrospective studies can evaluate disease management offerings, for example.



5. Multi-issue first call resolution

First call resolution once meant solving a customer's problem du jour within their first call to an insurer.

UPMC expanded on this idea by building a data registry yielding “a single source of truth” about members. Instead of using incompatible customer management systems throughout the company, UPMC developed one source of customer information, specific to each individual member and accessible to staff and members.

If someone calls to request a new ID card, a representative might see that care managers have been trying to reach that person and connect the two.

The same customer may want to arrange a flu shot, speak to a pharmacist, or report fraud. All this can be handled in one fell swoop.

6. Health assessments

UPMC's data scientists studied CMS-required health assessment surveys completed by new Medicare enrollees. They found 8 different combinations of 5 questions that flag people who need extensive care management.

UPMC now coordinates care for them out of the gate instead of waiting for costly claims experience to see who has complex needs. ●

PREDICTIVE ANALYTICS SHOW POTENTIAL TO SHORT-CIRCUIT PAY AND CHASE

by Darcy Lewis

In an ideal world, payers would identify fraudulent claims prepayment, avoiding expensive and frustrating pay-and-chase efforts later. Predictive analytics—sophisticated models built and continuously refined using the payer’s own data—may move a sizeable percentage of fraud identification much earlier in the payment cycle, leading many to hail predictive modeling as the next big thing in anti-fraud efforts.

“Predictive modeling creates a positive feedback loop where the data get better and the fraud prevention models more sophisticated,” says Louis Saccoccio, CEO of the National Health Care Anti-Fraud Association. “That’s why there’s a huge push for predictive analytics now.”

“More than 90 percent of advanced analytics focus on longitudinal data from claims at least 30 days old,” he says. “Payers have had a full view of their claims data but now we’re beginning to be able to add patient-side data. That will radically change payers’ field of view and



“What you learn post-payment today you might be able to use prepayment in the future.”

Louis Saccoccio, CEO, National Health Care Anti-Fraud Association

allow them to detect fraud much earlier.”

Golberg points to developments such as the Centers for Medicare and Medicaid Services’ new requirement that Medicare patients complete a health and wellness survey during their annual checkup. “Those surveys will begin to give you data,” he says. “For starters, was that patient actually seen? You can delve deeper from there.”

Other resources for increased pattern recognition include patient risk assessments, patient satisfaction surveys and telemetry. “Watch for things like a patient receiving diabetic medications and supplies but not providing glucose data to their provider,” Golberg says.

Golberg also cautions payers not to overlook social media or certain key websites as they build their models. “You’ll want to correlate with sites like StreetRx.com, a crowdsourced collection of prescription drugs’ street prices by date and location,” he says. “Or watch Twitter for comments about who is an easy doctor to get drugs from.”

Many payers are still working to take advantage of what’s currently available, let alone what’s coming. Saccoccio points to a proprietary NHCAA benchmarking survey in which 59 member companies responded to questions about using data analytics. When asked if their anti-fraud unit currently uses some form of data analytics, 83 percent said yes. But when asked if their special investigations unit uses prepay software, only 22 percent said yes.

Saccoccio expects that gap to close rapidly.

Consider these three points as you move towards implementing predictive analytics in your own organization.

Even major payers are still honing their predictive analytics strategies and systems. But in general, the best approach is to focus on how to gather additional types of data earlier in the process, says Mark Golberg, general manager of the provider, payer and ACO sectors at consultancy Recombinant by Deloitte.

Balance competing internal interests

Your top priority may be to prevent payment of fraudulent claims but recognize that colleagues have



“Predictive analytics are a fine line in terms of competitive advantage. Yes, all the payers are on the same side, but we’re also competitors.”

Lee Arian, staff vice president of program integrity and investigations at WellPoint

other, equally legitimate, concerns.

“Virtually every state has a prompt pay law and the most common time limit is 30 days, though many will make exceptions for open investigations,” says Saccoccio. “You’ll never have as much time as you want to analyze claims, so figure out how to make your process work with the prompt payments that keep providers and members happy.”

Plan to increase headcount

Simply put, more data will require more people. Golberg emphasizes that payers will need to add programmers, data scientists and consumer data strategists. But other scenarios are possible, even likely.

Lee Arian, staff vice president of program integrity and

investigations at WellPoint, is fielding a pilot predictive modeling project in Georgia prior to an enterprise-wide implementation planned for 2014. The pilot’s data allowed WellPoint to pinpoint the type of additional personnel it should hire.

“We knew we would need more employees but didn’t know the exact mix before the pilot,” Arian says. “We uncovered questionable payments, especially in the area of testing, so we need more clinical people to help us understand results and act upon them. Having more coders would help us know whether that MRI or lab test was really necessary.”

Share what you can

At least for now, expect that peers at other payers may not be able to provide the level of formal and informal sharing you may be used to.

“Predictive analytics are a fine line in terms of competitive advantage. Yes, all the payers are on the same side, but we’re also competitors,” Arian says. “We want our proprietary tool to have a perceived value in the marketplace, so we have to be careful what we share.”

But Golberg supports information sharing, both to smooth analytics planning and implementation and, as usual, to keep ahead of the fraudsters.

Saccoccio encourages payers to pursue predictive analytics sooner rather than later.

“The NHCAA believes all payers need to get on board with predictive analytics to make a meaningful dent in the fraud problem. What you learn post-payment today you might be able to use prepayment in the future,” he says. “It’s a matter of finding the right tool for your company and integrating the solution into your claim systems.” ●

LexisNexis® solutions for health care leverage identity and fraud identification analytics to help payers reduce improper payments, improve investigative and recovery efforts, and improve member outreach efforts through better identity related data. Our solutions help health plans address the pillars of the Affordable Care Act which are costs, quality and access.

