Health Care Payment Integrity through Advanced Analytics

BEN WRIGHT, AHFI
Sr. Solutions Architect
Security Intelligence Global Practice, SAS

SEPTEMBER 2017
Health Care Payment Integrity through Advanced Analytics

Introduction

Insurers have long been plagued by fraud, error, waste, and abuse in health care payments. The costs are huge – amounting to as much as 25 percent of payments made. Today’s data management and analytics platforms promise breakthroughs by incorporating comparative and behavioral data to predict as well as detect loss in all its forms. To explore the opportunities and how insurers can capitalize on them, IIA spoke with Ben Wright, Sr. Solutions Architect in SAS’s Security Intelligence Global Practice.

What’s most challenging about the health care payment landscape these days?

For starters, we’re in the middle of the fundamental shift from fee-for-service billing to bundled payments and accountable care organizations (ACO) with the intention to link payment to successful treatment outcomes and efficient health care delivery. Meantime, the demographics of the covered base are changing as more people have access to health insurance, including populations that payers do not have good risk profiles for. And then there are continuing health policy changes, as the risk adjustment support that the government has been providing in the state and local exchange markets is phased out. That affects the Medicaid and commercial markets in unanticipated ways. For example, we’ve learned that significant premium increases slated to take effect in Medicare Part B are going to cascade to the states for dual-eligible Medicaid recipients, adding additional costs to overburdened state budgets. So for payers, claims administrators and Managed Care Organizations, the landscape is extremely challenging. Cost management is once again front-and-center, and that’s driving increased focus on payment integrity.

Please define payment integrity and its business objective.

Health care payment integrity (PI) means that each claim is paid correctly, that payment is made by the appropriate party to an appropriate party, and that payment is for the treatment of an eligible individual according to the plan-of-benefits contract. The payment must be neither in error nor in duplicate, and it must be absent of wasteful or abusive practices. That covers a lot, but the most important thing to recognize is that payment integrity is not an isolated step; it doesn’t happen only at claims adjustment time. Payment integrity, or the lack thereof, is determined by an end-to-end business process beginning with the definition of a plan of benefits and enrollment of members, right through claims processing, payment, and customer service. Success with payment integrity depends on the accuracy, availability, timeliness, and organization of all the data associated with this end-to-end process. The business objective is accurate payment, and cost control through loss prevention and elimination of wasteful, duplicative or unnecessary administrative processes.

How big is the opportunity for improvement in payment integrity?

If you look at the numbers conservatively, the estimated costs of fraud, waste, abuse, error, and improper payments haven’t changed much since the National Health Care Anti-Fraud Association was founded and started tracking them in 1983. True fraud has always been estimated by many sources at 3 to 10 percent of total health care payments. Waste, abuse, and error estimates vary from a low of about 15 percent to a high near 30 percent. CMS finds that as
much as 20 percent of Medicare payments are lost in waste, abuse, and error. If we look across those numbers, somewhere between 25 percent and 30 percent of the total health care bill can be attributed to losses across the full spectrum of fraud, waste, abuse, and error.

It’s clearly better to prevent inaccurate payment from going out in the first place than to try to recover it later. True fraud is often perpetrated by actors who may not have much to do with the health care process other than preying on it. The motive is simply to exploit any gap that allows unjust enrichment. To the extent that business rules can be developed around true fraud detection, those rules will rapidly become ineffective because the fraudsters, if not caught, will change behavior and seek out other gaps in the process. Error, waste, and abuse are different. There’s a wide variety of actors and causes, and many times you can correct things, even billing abuse, with education. A billing provider may not be aware of their difference from their peer group or their anomalous results and payment processes may suffer from data quality gaps, errors, and process defects that undermine accurate payment.

Interestingly, error and inefficiency seem to be emerging as the number one loss category, a larger component than is usually recognized. Fraud gets the headlines when there are huge dollar amount convictions, but there aren’t that many large cases overall and a lot of those dollars are never recovered. Errors cost money and waste resources continuously until detected and corrected. Those losses are preventable and increasingly predictable. When payers capture detailed, granular data about payment processes, then advanced analytics can have immediate impact on improper payments because the payer has complete control over the payment process. Processes such as group implementations, coverage policy changes, and new clinical claims policies all influence payment and may introduce defects that are not discovered by baseline testing of systems releases. Happily, many of the same analytics techniques applied when focusing on fraud detection (anomaly detection, trend analysis, regression, and predictive techniques) can identify gaps in payment integrity when the payment process is examined in an end-to-end holistic way and when the analysis includes data about relevant internal processes captured during service operations.

**How is the Payment Integrity Process Changing, or How Should It Change?**

Major business changes are underway that will result in a laser focused re-examination of payment processes. The largest health payers adjudicate millions of submitted health transactions every day, and as consolidation in the industry continues there will be significant advantage to be gained through improvement in payment and other service operations processes. Payment integrity analytics wins from two angles. First, the organizations will gain from using analytics to assess the effectiveness of each payment process as they strive to leverage the scale of their merger. Second, the merging of these operations creates significant, additional complexity. As the organizations attempt to optimize combined processes for efficiency and cost effectiveness, advanced analytics are necessary to ensure that payment integrity is maintained while enhancing customer service.

There’s a particular challenge around the Special Investigations Unit (SIU), traditionally the focal point for fraud detection. The SIU cannot marshal resources on its own to stand up robust analytics that address the end-to-end payment integrity process, but the company can. And the SIU will benefit from being part
of that larger process, not a separate analytics operation. The enterprise data governance process and enterprise data repositories should serve all forms of loss prevention through a comprehensive, shared advanced analytics layer. It’s no longer fraud analytics in one box and everything else in Service Operations or in Informatics.

So how do data and analytics play in improving the process?

With today’s big data environments, we can bring together much more contextual information—from provider contracts and company policies to comparative behavior and performance data as well as external data that helps assess risk and differentiate behavior—to surround the services and claims transaction data. With a robust, advanced analytics platform, we can detect patterns and anomalies as never before, and improve payment decisions. From the modeler’s standpoint, the richer data sets enable better model “training,” so analytical models get smarter faster and the whole payment integrity process is improved. I think we’re on the verge of dramatic breakthroughs in payment integrity performance and in our ability to reduce false alerts.

Let’s start with fraud as fairly familiar territory. The ultimate goal is to detect fraud prior to payment. But we’ll never get to the point where the payment denial decision can be made with 100 percent confidence without human review, because fraud hides. Fraud masquerades as something legitimate. So we can improve detection, but we’ll always have false positives, and we’ll always detect some fraud after the fact or not at all. But let’s try to detect it as early as possible.

Fraud detection improves when we look across the behavior of individual members, providers, and groups of similar providers—or groups of similar conditions, or groups of similar treatments, or groups of similar payments—and we fold in clinical data such as test results, even in non-traditional areas such as neurology. If we have a provider regularly submitting claims for nerve conduction tests, but the results are identical for a significant number of patients, there’s a problem. Perhaps the person submitting claims is taking a shortcut by copying data. Or perhaps there’s real fraud—no tests done and no real patients. That’s a simple example of what we can notice with contextual data and basic analytics.

Here’s a more challenging example in the error category. Payment integrity spans a process that begins with the account sale, plan setup, enrollment and finishes with call and claim setup. At a major health payer, this is a high-volume and labor-intensive process that repeats on January 1 for thousands of groups and may require over 1,000 payer staff to accomplish. In January, a high incidence of errors related to a particular subset of Medicare claims was observed. Data about the members being enrolled, the employees enrolling them, the system actions they performed, the relevant account plan structures, and the types of errors reported to the call center were combined and analyzed. Summary statistics methodologies and logistic regression techniques were applied.

One result was intuitive—employees who handled more Medicare cases were more accurate. Another was less intuitive—employees with the lowest error rates took the longest time and performed many more steps on each transaction so they appeared to be less efficient. Process data revealed that those employees were consulting more sources, making extra checks, and soliciting more assistance from colleagues. In reality, they were better at navigating a complicated
data and systems infrastructure that suffered from data quality and timing failures for this particular business type. Staff who were less experienced didn’t recognize the need to take additional steps and payment errors ensued. The error-reduction solution included improving the timeliness and completeness of eligibility information, improving the workflow, and automatically routing the most complex cases to the more experienced employees.

**What special challenges do analytics professionals face when developing and deploying models and applications for payment integrity?**

The biggest challenges relate to data quality and need to be addressed through enterprise data governance and enterprise data management. Inconsistent and redundant data is prevalent when payers have fragmented and overlapping core systems, or that may have recently undergone a merger or acquisition or integrated combined businesses. Interestingly, organizations with more analytics “verticals” — business areas with their own data and analytics professionals — also contribute to this condition. Data may be accurate for its local purpose but different across the organization. So the challenges are integration and disambiguation. Furthermore, if analysts and modelers don’t have – or have access to – business background and subject matter expertise, they can trip on these data issues. In order to solve these problems, organizations are adopting data management software tools to ensure an accurate source of truth before applying advanced analytics. Another problem is data timeliness and detail. A lot of the data traditionally available for analytics was in warehouses, where it had been manipulated, altered or summarized and was as much as a month old or older. Payment integrity analytics needs timely operational data, not just the usual transaction data associated with eligibility and claims, but also business data about costs, as well as clinical data about services and outcomes typically managed by medical informatics. To address this, analytics professionals should ensure that their analytics implementation leverages unadulterated operational data close to its point of creation.

**Who are the major stakeholders in payment integrity?**

I count three, and the third is missing in many organizations.

First is the CFO, who wants to minimize cost and risk. If the company is leaving 20 percent or more of medical payments on the table, the CFO should be very interested. If the CFO understands the potential to lower cost through a combination of data management, advanced analytics, and process improvement, then she can be the driver behind payment integrity initiatives.

Second is the CIO, especially if responsible for both data management and analytics. The CIO has the opportunity to bring together operational, clinical, and business data and analytics to integrate the payment integrity process and dramatically improve its performance.

Too often missing in action is an owner of the payment integrity process. People are responsible for parts of the process, but no one is in a position to oversee and improve it end-to-end. In one company, the payment integrity process benefited significantly, if indirectly, from an end-to-end examination of process.
effectiveness focused on reducing process errors. The head of operating effectiveness took on the role, but did so in the name of “quality”. If your organization has a senior executive in an analogous process improvement role that may be the stand-in until payment integrity emerges as a C-suite role in its own right.

**What are the top three things stakeholders should know and do with respect to payment analytics?**

First and foremost, recognize the size of the opportunity to prevent loss and manage cost across the board – fraud, error, waste, and abuse. Data and analytical platforms are available today to make a real difference, finally folding in the contextual and behavioral data to drive predictive insight, so choose a recognized leader in analytics. These advanced analytics platforms can be hosted solutions and still provide high performance tools that are accessible across the enterprise. Payers can leave a lot less money on the table.

Second, address your organization’s data issues through enterprise data governance, and related software toolsets for enterprise data management that support the discovery and cataloging of data across the enterprise. It’s an investment in performance improvement and future agility for all facets of the enterprise. This is an area where “one and done” definitely beats the nuance of “28 flavors”. I earlier stressed the importance of data quality, but keep in mind that the definition varies. Big data analytics applications don’t need perfect data – they need rich data sufficient for the analysis at hand. So even while you’re making headway resolving and integrating operational data, you can already be putting new analytics to work.

Third, treat payment integrity as an integrated end-to-end business process. Measure it and make sure someone is responsible for it. Also deploy data and analytics technology platforms that can serve the entire process, not just pieces of it. High performance, large data stores — think Volume, Velocity, Variety, and Variability — require a robust analytics layer and powerful but accessible tools that deliver insights with power and data visualization. With today’s technology and analytical methods, you can move from retrospective analysis to predictive detection and influence payment decisions in real time.

**Please sum up the case for payment integrity analytics.**

Traditional legacy approaches to payment integrity focused on investigation and prosecution of fraud by dedicated business units isolated from the mainstream payer organization, absent at the table when data and analytics project funding are on the annual enterprise planning agenda and often viewed as a compliance and reporting organization. The most important cases got the attention, but they were limited in number, and retrospective recovery – or “pay and chase” – doesn’t work well. If you’re lucky, you recovered 25 cents on the dollar, or may have paid a 20 percent fee to a recovery partner. There was little incentive to get to root causes and prevent fraud in the first place.

Today, payers have unprecedented ability not only to prevent fraud, but also to tackle error, waste, and abuse on a large scale through effective deployment of advanced analytics. They can take preventive measures where the greatest losses are accumulating,
starting with basic error. They can find savings, improve processes, and solve problems that were too small for the SIU to address. Those savings can add up quickly and improve the bottom line in turbulent times.

And the SIU can benefit from the same analytics infrastructure by identifying, investigating, and making higher-value referrals to regulators and law enforcement. This is true because the SIU professionals can apply a unique combination of skills—clinical, legal, claims process, and law enforcement—with advanced analytics to ensure that those who intentionally perpetrate fraud without regard for patient safety and financial wellbeing have a positive outcome; jail time.

Additional Information

To learn more about this topic, please visit http://sas.com/paymentintegrity.
About the Interviewee

BEN WRIGHT, AHFI

Ben Wright is a Senior Solutions Architect in the Security Intelligence Global Practice at SAS, Ben provides support in planning, marketing and implementation of health fraud detection, investigation management and payment integrity solutions for State Government and Commercial Health Payer customers. Ben has worked in pre-payment fraud detection, applied data analytics, and payment integrity process support for over 25 years and has been a SAS software user for over 30 years. Prior to SAS, Ben worked at Cigna, Inc., in Service Operations, at Booz | Allen | Hamilton, as a Sr. Associate in Cloud Analytics and at Aetna where he held various roles in IT Application Development, Project Management and SIU analytics for over 30 years. Ben holds a Bachelor of Arts from Dartmouth College and did post graduate studies at the University of Virginia.