Research Article

iMedPub Journals
http://www.imedpub.com

Journal of Health & Medical Economics
ISSN 2471-9927

2016
Vol. 2 No. 2: 11

DOI: 10.21767/2471-9927.100017

The Potential Savings of using Predictive Analytics to Staunch Medicaid Fraud

Parente ST, Oberlin S, Tomai L and Randall DO

Department of Finance, University of Minnesota, CSOM, Minneapolis, MN, United States

Corresponding author: Parente ST

sparente@umn.edu

Department of Finance, University of Minnesota, CSOM, Minneapolis, MN, USA.

Tel: 6122818220

Citation: Parente ST, Oberlin S, Tomai L, et al. The Potential Savings of using Predictive Analytics to Staunch Medicaid Fraud. J Health Med Econ. 2016, 2:2.

Abstract

Health care fraud is a major policy concern. In this paper, we report the results of applying fraud and abuse analytical detection technology with a predictive algorithm to identify and extrapolate the extent of Medicaid fraud and abuse in terms of prevalence and expenditures from 2008 to 2012. Using Medicaid claims from the State of Louisiana, we estimate approximately $61 million per year in potential savings from the initial entry of the program. Long-term savings are estimated to be $97 million per year by 2019. Implementation of this technology, and the associated technology, can begin immediately in order to start realizing these savings.

Keywords: Health insurance; Medicaid; Fraud; Health economics; Physician payment

Received: December 18, 2015; **Accepted:** February 09, 2016; **Published:** February 15, 2016

Introduction and Background

In an era focused on minimizing growth in health care spending, the need to identify and eliminate fraud and abuse in the Medicare and Medicaid programs is top of mind for many policy makers. While the annual cost of fraud and abuse is not known, improper payments to Medicare and Medicaid were estimated at $75 billion in 2010, a value that escalated to $98 billion in 2011 [1]. As these programs continue to grow vis-a-vis the aging of the population, increasing the number of Medicare beneficiaries, and the implementation of the 2010 Patient Protect and Affordable Care Act (PPACA), increasing Medicaid beneficiaries, the need to detect and monitor fraudulent activities will be even more pertinent. As the PPACA unfolds, the United States (US) is experiencing the greatest expansion of the Medicaid program since its creation in 1965 [2]. An estimated 16 million new Medicaid beneficiaries will be added to the state-federal health care program for low income Americans. Total program enrollment is estimated to increase from approximately 55 million in the current fiscal year to over 78 million by 2019 [3]. Federal and state government spending will follow, increasing from $490 billion to $890 billion during the same time period; a net increase of approximately $400 billion. Additional and unnecessary spending is also anticipated if policies and procedures around fraud and abuse remain status quo. Industry experts estimate Medicaid fraud will cost upwards of $1 billion for the current fiscal year - a number that could double by 2019 [4]. As Medicaid expands, there is an opportunity for those responsible for its implementation and oversight to take a more aggressive approach to detect and mitigate fraud and abuse.

The Medicaid and Medicare programs differ in many ways, including how the programs are designed, which subsequently has an impact in understanding the areas in which fraud and abuse can occur. The Medicaid program was designed as a federal-state partnership, with the federal government providing a formula to match funds, and state governments implementing and overseeing the program. In response, many states have chosen to work with a number of private firms to administer Medicaid to providers (hospitals, physicians and other ancillary providers) that have contracts to provide health care to Medicaid beneficiaries in that state [5]. As the Medicaid program expands, states are also anticipated to utilize organizations such as Centene and Molina to help provide IT, administrative and business processing services [6]. Combining the need to interact and monitor thousands of small and large vendors, in an already complex bureaucracy, with an increase in beneficiaries and spending, the probability that some claims will be fraudulent is almost an absolute certainty.

Recognizing the need for stronger oversight, the Department of Health and Human Services, in conjunction with the Department of Justice, established a Health Care Fraud Prevention and enforcement Task Force Action Team (HEAT). HEAT creates a forum for relevant agencies to collaborate and coordinate fraud mitigation efforts. The most recent efforts by HEAT resulted in over $3 billion in judgments and settlements for fraud and abuse,

with approximately $2.4 billion being returned to the Medicare Trust Funds and almost $900 million being returned to the U.S Treasury for Medicaid [4]. The Justice Department and HHS estimated that their fraud efforts had a return on investment of $7.90 returned to Medicare and Medicaid for every dollar spent. They also viewed technology as an important tool, and leading contributor to HEAT fulfilling its mission [4].

The use of technology, specifically the use of advanced analytics and predictive modeling to identify and prevent a fraudulent transaction, was pioneered by the financial services industry over twenty years ago. At that time, credit card fraud was accelerating with the use of electronic payment technologies. Implementing fraud prevention analytics resulted in a 50% reduction in credit card fraud within five years of market usage [7]. Applying financial services predictive analytics to health insurance claims is appropriate due to the similarities in transaction payment systems. For example, credit card and health insurance claims systems each rely on a combination of debits and credits for accounting and both use standard code sets to record the purchaser and vendor (e.g., the medical provider and payer for health care) associated with a transaction. The difference is the use of algorithms to identify aberrant behavior that is typically associated with fraud or abuse. For example, the algorithms used to generate the results in this study identified a mid-wife knowingly billing for a surgical procedure that was outside the mid-wife's scope of practice for a Medicaid beneficiary. In this case, the analytics could be used in real-time to stop (or at least delay) payment to the mid-wife until the transaction is verified.

Another difference is the ability to detect false positives and false negatives. Algorithms are not perfect and could identify a non-fraudulent transaction as fraudulent. Financial institutions will stop payment immediately to prevent a loss of funds. In health care, real-time detection is the goal, but will need to include processes to protect both patients and providers. Today, since most claims are filed hours, days or a sometimes month after a service is performed, a denied or investigated claim does not restrict a patient from receiving care. In addition, many of the false positives identified are due to inaccurate billing practices which may prevent providers from getting paid for services rendered. Finding solutions for marginal errors must be a part of any fraud and abuse technology.

As Medicaid expands, the need to identify and mitigate fraud and abuse is necessary, especially for federal and state policy makers charged with overseeing its implementation. The purpose of this study is to use fraud and abuse technology applications to estimate the potential of Medicaid fraud prevention and the potential dollars saved through the use of these applications. Three specific questions will be addressed:

1. What is the probability of fraud among Medicaid providers?
2. What Medicaid savings can be generating after identifying the fraud potential?
3. How do different modeling techniques impact the ability to detect potential fraud and to estimate meaningful savings in a state Medicaid system?

Research Design

Louisiana Medicaid claims data was used for this study. The state Medicaid program represents roughly a million non-elderly covered lives. Four years of data were analyzed and included all segments of Louisiana's Medicaid program as well as Provider, Beneficiary and Beneficiary Eligibility files. Data was collected from July 2008 to July 2012, at the procedural level for all claims analyzed. Only fee-for-service (FFS) claims for specialty physicians, pharmacy spending and home health reimbursement were selected for modeling.

Potential for note or side bar

FFS claims data for specialty physicians, pharmacy spending and home health reimbursement were chosen for two primary reasons period

(1) Ancillary provider services, including durable medical equipment (DME), and prescription drug services have grown dramatically in the last decade, exhibiting rates higher than overall Medicaid per-capita spending, and have been of particular interest to state and federal policy makers [8].

(2) They are reimbursed on a FFS basis, which constitutes the majority of spending by state Medicaid systems [9].

Once the data were collected, samples of providers were randomly selected and scored with a generic or custom predictive model. The scores were then used to estimate the probability of fraud.

The generic and custom models were developed by Fortel Analytics, LLC, with funding from both the Department of Health and Human Services and The Centers for Medicare and Medicaid Services. While the detailed algorithms of each model are considered trade secret intellectual property both apply Bayesian and non-parametric statistical methods to health insurance claims to estimate the probability of fraud. Using a non-parametric approach allows for the independent assessment of multiple dimensions in a given claim (e.g., the beneficiaries' attributes and care, and the providers' preferences and treatment patterns, provider specialty and geography). The outputs are then translated into probabilistic scores, which estimate the likelihood that one or more of the dimensions shows unusual, abnormal or fraudulent behavior.

For a predictive model score to be meaningful, it is first necessary to calculate a proprietary non-parametric statistic that measures the dispersion for predictive variables relative to a threshold value. This statistic estimates the deviation from normal cohort behavior (the threshold value) and determines if a behavior is "typical" of other participants in their cohort group or if it is "abnormal" [10]. Previous studies have shown following this approach limits inaccurate fraud detection including both false positives (where a suspected health care fraud was a legitimate service) and false negatives (where there was a failure to identify a fraudulent activity) [11].

Once the threshold values are determined, each provider is given a probability score ranging from 0 to 100, with higher values indicating higher payment risk and lower values indicating lower payment risk. Therefore, the highest-score values have a higher

probability of fraud or abuse. These probability estimates can then be used to compare the relative performance, or risk, across different geographies, provider specialties, industry segments, or as in this study, to estimate the potential cost savings [12].

There are six steps to estimating the cost savings potential if fraud and abuse technologies are utilized.

1. Identify the total share of payments at-risk. This value will then be used as the foundation for calculating the share of potential fraud that can be recovered through the use of predictive modeling.
2. Determine the level of risk that will be considered actionable by an agency. Credit card fraud detection usually operates with risk probability of 90 or greater. In this study, high risk is defined as Tier 1 (95 to 100) and Tier 2 (90 to 95). Once the actionable level of risk is determined, the percentage is then applied to the total payments at-risk resulting in a revised at-risk payment amount.
3. Apply a discount factor (Non-actionable Issues) to account for non-actionable issues such as provider misclassification, indeterminate eligibility for provider payment and false positives, among others. This measures the accuracy of the fraud detection methodology. As accuracy improves (through the incorporation of real-time data), the discount factor decreases. The discount factor is then applied to the revised at-risk payment, modifying this value further.
4. Apply a second discount factor (Actionable Issues) to account for actionable issues such as coding errors resulting in inappropriate billings. The Actionable Issues discount factor will also decrease as providers improve their billing processes. For the credit card industry, the elimination of paper transactions was a major step forward. Health care claims billing is on a similar path with more robust business analytics and electronic health records, but will need fraud enforcement activities to detect and minimize errors.
5. The final result is the total cost saving potential that can be achieved by using fraud and abuse predictive models.
6. To assess whether different types of predictive modeling have an impact on the ability to detect Medicaid Fraud, both the generic model and custom model were utilized.

Generic model

The Generic Model was constructed using Medicare claims data and contains all variables known to be predictive of fraud, waste and abuse. While the details are patent protected, the model has been validated using a large Midwestern state's Medicare population with results published in a peer reviewed journal [12]. For this study, the model was repopulated with Louisiana data, and the results were reviewed and validated by external expert investigators.

Custom model

The custom model starts with the generic model and modifies it based on additional variables such as contracting, specialties, and practice location that were not available in the generic model. The more variables identifying common behavior and relationships, the greater signal a predictive model can use to help identify and prevent fraud. Similar to the generic model, random samples of the highest scoring (95 and higher) at-risk providers were sent to an independent group of reviewers to evaluate the effectiveness of the scores.

External reviewers were a group of independent health experts comprised of nurses and health insurance claims specialists. They were engaged to conduct independent validation reviews of the model outputs including provider scores, reason codes, and a detailed claims and procedures historical review [13]. When necessary, additional statistical analyses were also conducted to quantify and support the external reviews. All claims reviewed were paid for and complied with existing policy rules, fraud edits and audits in place.

Results

We focused on three questions in this study

(1) What is the probability of fraud among Medicaid providers?

(2) What Medicaid savings can be generated after identifying the fraud potential?

(3) How do different modeling techniques vary in estimating potential fraud and potential costs savings from using fraud prevention/detection technology? Answers to these questions can be found in **Tables 1-3.**

Table 1, 2019 Louisiana Medicaid Fraud Probability Risk, summarizes the potential for Medicaid fraud by tier and major at-risk category (e.g., payments, providers and claims) for Louisiana in 2019. Using the custom model, approximately $1.6 billion of claims payments are at-risk for fraud. Roughly $500 million, or almost 32% of payments, fall into the highest risk segment (95-100). This represents 11.6% of the Medicaid provider population and approximately 32% of physician claims. For this tier (Tier 1), the recommended action is to hold payments until further verification is complete. Using the same probability risk score for credit card fraud of 90 or above, approximately 22.3% of providers are at-risk for fraud, increasing potential payments at-risk to

Table 1 2019 Louisiana medicaid fraud probability risk.

Tier	Fraud Probabilty Risk Range	At-Risk Payments (000,000)	Share of Total Dollars At-Risk	Share of Providers At-Risk	Share of Claims At-Risk	Recommended Action
1	95 - 100	$504	31.6%	11.6%	32.1%	Hold Payments
2	90 - 94	$233	14.7%	10.7%	18.2%	Research/Watch List
3	80 - 89	$385	24.1%	24.3%	26.3%	Educate
4	<80	$471	29.6%	53.4%	23.4%	Make Payment
Total		$1,593	100.0%	100.0%	100.0%	

Table 2 Potential cost savings to Louisiana's medicaid program.

		Current	Long-term
Description of Analysis		Fiscal Year	2019
Total payments at-risk		$1.0 billion	$1.6 billion
% Share of at-risk dollars in Tiers 1 and 2		46%	46%
Revised payments at-risk (Tiers 1 and 2)		$0.44 billion	$0.7 billion
Discount Factor (Actionable Issues)	(Adjustments for inappropriate billing)	~32%	~32%
Revised payments at-risk (Tiers 1 and 2)	(factoring in discounts for actionable items)	$299 million	$478 million
Discount Factor (Actionable Issues)	(Adjustments for inappropriate billing)	~20%	~20%
Revised payments at-risk (Tiers 1 and 2)	(factoring in discounts for actionable items)	$238 million	$381 million
Total Net Annual Savings Opportunities		$61 million	$97 million

Table 3 Comparing a generic and customized model in potential fraud prevention.

	Custom Model				Generic Model			
Fraud Probabilty Risk Range	Share of Providers At-Risk		Share of Payments At-Risk		Share of Providers At-Risk		Share of Payments At-Risk	
	%	Cum. %	%	Cum. %	%	Cum. %	%	Cum. %
95 - 100	11.6%	11.6%	31.6%	31.6%	7.0%	7.0%	21.6%	21.6%
90 - 94	10.7%	22.3%	14.7%	46.3%	8.2%	15.2%	14.7%	36.3%
80 - 89	24.3%	46.6%	24.1%	70.4%	21.8%	37.0%	26.7%	63.0%
<80	53.4%	100.0%	29.6%	100.0%	63.0%	100.0%	37.0%	100.0%

more than $730 million. While more than 50% of physicians have a low fraud probability risk (<80), giving the green light to make a payment, this represents only ~30% of total dollars at risk (~$470 million).

A total payment at-risk does not represent the potential cost savings to Medicaid. **Table 2** illustrates the estimated cost savings to Louisiana's Medicaid program for the current fiscal year and in 2019. If Louisiana implements the custom Medicaid fraud and abuse model, the state is estimated to save approximately $61 million in the current fiscal year and $97 million by 2019.

In following with the four steps of the cost savings methodology, the total payment dollars at-risk for fraud are $1 billion (current fiscal year) and $1.6 billion (long-term). For this example, the level of risk for Louisiana Medicaid deemed to be actionable (meaning the state would take action to prevent or mitigate fraud) was defined as the combined fraud probability risk scores for tiers 1 and 2, which is approximately 46% (31.6% in tier 1 and 14.7% in tier 2). The total payments at-risk were then reduced by 46%. Two additional discount factors (Non-Actionable and Actionable Issues) were estimated at 32% and 20%, respectively. These percentages were then applied to the at-risk payments, decreasing the total dollar amount and resulting in a revised at-risk payment. As mentioned, the discount factors will decrease with improvements in modeling, technology and billing processes ,resulting in higher costs savings. Putting this into perspective, in 2019, the $97 million cost savings (due to fraud prevention) would yield 5.7% (97M/1.7B) of allowed charges paid by the state or federal government.

To assess if there is a difference in the probability of fraud and cost savings potential by using different predictive models, a generic and custom model were employed. **Table 3**, Comparing a Generic and Customized Model in Potential Fraud Prevention, summarizes key outputs from the models and demonstrates the advantage of creating a customized model for fraud detection.

When comparing the cumulative percentage of providers at-risk for fraud in the high risk tiers (90-95 and 95-100), the generic model only identifies 15.2% of providers at-risk compared to the 22.3% with the custom model. This translates to a 10% decrease (46.3% compared to 36.3%) in the potential payments identified at-risk for fraud.

Discussion and Policy Implications

Medicaid expansion will bring about many and varied policy challenges to state and federal policymakers as enrollment and costs increase. Historical trends suggest that with these increases, fraud and abuse will surely follow. Also, as states continue to relying on outside vendors for support, the possibility of fraud is only amplified. This study not only demonstrates how the use of predictive modeling with fraud detection algorithms can assist-at least one state, Louisiana, in detecting fraud and abuse, but also has the potential to reduce Medicaid programmatic costs by more than HEAT's estimate of $1 Billion.

While some believe that the use of claims data to detect cost savings from fraud underestimates the true problem, the use of predictive modeling is a starting point. In this study, we used two models-a custom model and generic model-and while the custom model showed higher rates of return, the generic model was still able to identify approximately 36% of claims payments at-risk for fraud. Predictive modeling-even with claims data-can make fraud prevention a reality.

It is important to note that there are alternatives to using fraud prevention technology to contain costs; specifically changes to the payment system. As mentioned, a FFS payment environment is more conducive to fraud and abuse compared to capitation, as the provider has more control over cost and coding. This is

particularly important as the industry moves to accountable care organizations, with more parties involved (e.g., hospitals, physician groups, insurers) and with multiple payment methodologies (e.g., FFS, shared savings, capitation, etc.).

In July of 2012 (after this study), Louisiana converted its Medicaid program from fee-for-service to managed care. Two of the managed care plans currently in Bayou Health are operating on a shared-savings model (which continue to use a FFS platform), while the other three are fully capitated. Preliminary results indicate that the capitated plans are working better at lowering health care costs and improving quality. From this, one can presume that unnecessary spending due to fraud is also less, a parameter that will need to be tested in the future.

Even under a capitation arrangement, the use of predictive modeling to find fraud, abuse or waste could be used to adjust and/or reduce the Per-Member-Per-Month (PMPM) payment levels. For those states embarking on full scale capitation contracts, but which maintain fee for service like encounter data, this could be an effective tool to identify inefficiencies and improve quality of care.

The results from this study suggest that advanced analytics and varied predictive modeling techniques have the ability to identify potential fraud issues before they become a problem, often resulting in significant cost savings. The return on investment of current HEAT efforts gives ample justification for using fraud detection and mitigation techniques. Both the custom and generic models used in this study further support their studies by showing the possibility of even higher rates of return. As state Medicaid programs begin to implement Medicaid expansion under PPACA, the importance of finding program savings and controlling costs take on added significance. Predictive modeling is one tool to help cope with the many implementation challenges to come.

References

1. Health Affairs Brief (2012) Eliminating Fraud and Abuse. New tools to reduce improper Medicare and Medicaid payments promise savings, But many implementation challenges remain.
2. Public Law (2010) The Patient Protection and Affordable Care pp: 111-148.
3. Office of the Actuary (2010) Centers for Medicare and Medicaid Services Department of Health and Human Services, United States.
4. HEAT Report (2012) Office of the Inspector General, HHS, United States.
5. Randall D, Parente ST (2012) U.S. Medicaid managing care markets: explaining state policy choice variation. Insurance Markets and Companies: Analyses and Actuarial Computations 3: 35-49.
6. Rosenbaum JD, Sommers BD (2013) Using Medicaid to Buy Private Health Insurance - The Great New Experiment? NEJM 369: 7-9.
7. The Nilson Report (2006) Credit Card Fraud - US pp: 1-10.
8. Miller GE, Sarpong EM, Banthin JS (2012) Recent Trends in Prescription Drug Use and Expenditures by Medicaid Enrollees.
9. Kaiser State Health Facts (2013) Medicaid Benefits: Medical Equipment and Supplies. Kaiser Family Foundation.
10. A peer group is defined as a group of members of the same dimension, including but not limited to healthcare claims or procedures, providers or of the beneficiary. For example, a peer group for providers might be their medical specialty, such as pediatrics or radiology.
11. Non-parametric techniques do not rely on data belonging to any probability distribution. Non-parametric statistical techniques also do not assume that the structure of a model is fixed.
12. Parente ST, Schulte B, Jost A, Sullivan T, Klindworth A (2012) Assessment of Predictive Modeling for Identifying Fraud within the Medicare Program. Health Management, Policy and Innovation 1: 8-37.
13. Model attributes responsible for a high-scoring provider are designated as model score reason codes (2012) The top reasons for the calculated score are presented to investigators to aid in their review process.