INTERNATIONAL INSTITUTE FOR ANALYTICS™

RESEARCH BRIEF
RESEARCH & ADVISORY NETWORK

Fighting the Rising Tide of Medicaid Fraud

JOHN MAYNARD
Principal Industry Advisor, SAS

TOM WRIGGINS
Principal Industry Advisor, SAS

ROBERT MORISON
Senior Advisor, IIA

JUNE 2022

Discussion Overview

Medicaid fraud has jumped dramatically in the era of COVID, as increasing complexity of delivery and payment models, along with increased funding, has created openings for fraudsters, including organized crime. States must respond by accelerating their deployment of big data, predictive analytics, and integrated technology platforms to manage Medicaid programs and prevent fraud. What's at stake? Not just cost control and taxpayer money, but health outcomes and equity for all recipients. To explore these challenges and opportunities, IIA spoke with Tom Wriggins and John Maynard, both principal industry advisors at SAS.

How has the COVID-19 pandemic affected Medicaid fraud?

Tom: The problem of fraud in government assistance programs exploded in 2020 and has continued to grow during the COVID public health emergency. In 2021, improper Medicaid spending hit a record high. According to the Centers for Medicaid & Medicare Services (CMS), improper payments totaled $98.72 billion, over 21% of total payments and more than a $10 billion increase over 2020.[1] Changes to Medicare and Medicaid rules due to COVID certainly have made things worse.

The consensus among states, the CMS, and the U.S. Health and Human Services Office of Inspector General is that loosening of program rules in response to the COVID pandemic resulted in rapid fraud growth across Medicaid, Medicare, and commercial insurance. The Medicaid program was already complex given states' ability to design their own programs, along with eligibility expansion and demonstration waivers. Fraud prevention is even more complicated now as a result of the heavier penetration of commercial insurance into Medicaid managed care in many states; the development of managed care models for dual-eligible people receiving both Medicare and Medicaid; and increases in value-based payment (VBP) models. In many ways, transparency has suffered.

John: Let me expand on that. Differences in Medicaid across states have only grown in the past several years. States began under a fee-for-service model where providers treated patients and billed the state for those services using a fixed fee schedule. However, nearly every state now has some form of a Medicaid managed care at-risk model where recipients are enrolled in private plans that agree to coordinate health care services and cover costs based on monthly capitation payments set by actuaries. Medicare now also offers managed care plans, even for those dual-eligible patients. These plans can take various forms and cover different groups of recipients. Collectively, this has only increased the complexity of the Medicaid and Medicare systems, and states don't always hire staff who truly understand those complexities.

As a former Program Integrity Director for a large state Medicaid agency, I find that all of these factors have increased the challenges of attempting to control fraud, waste, and abuse (FWA). When I took over program integrity, our FWA analytics were still quite primitive, and the team was still focused on fee-for-service providers and payments. However, nearly half

[1] https://www.cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/Medicaid-and-CHIP-Compliance/PERM/PERMErrorRateFindingsandReport

the payments were being made to commercial payers acting as Medicaid managed care health plans. While the state's contract compliance team was focused on patient health outcomes and emerging VBP models, nobody was really looking at how effectively FWA was being combatted in Medicaid managed care. As I began shifting our focus there, it quickly became clear that the updated federal FWA rules for managed care extended beyond the capabilities of the commercial payers' traditional special investigative units (SIU) as well.

Getting a handle on this complexity is incredibly important for state Medicaid programs. States must watch both fee-for-service and managed care plan networks now. I've noticed many state staff who wrongly thought fraud was not a problem in managed care. These health plans are paid a monthly "at risk" capitation payment for each category of patient to cover all the costs of their care. If the managed care plans cannot contain costs, the assumption is that the risk passes to them and not the states. However, FWA increases the total cost of care for all patients and thus the next year's capitation rates. As a result, if managed care plans are ineffective at program integrity, the extra costs are ultimately passed back to the states. "At risk" doesn't mean exactly what states might believe.

Tom: That's an excellent point. Traditionally in the commercial health care insurance space, the focus has been on payment integrity with less direct emphasis on fighting fraud. Commercial payers are reluctant to get their names in the newspaper and sometimes even to acknowledge that they are susceptible to fraud. The addition of health care exchanges and rapid growth of Medicaid managed care meant more complex provider contracts and more errors by the insurers' claims processing systems. Errors include many overpayments, as we continue to see in our advanced analytics work at SAS.

Meanwhile, the operations areas in most commercial payers utilize multiple payment integrity contractors, some working on a contingency basis from the overpaid claims they recover. States may not understand this model and how it affects their total cost or the minimum-loss-ratio reporting required by CMS for both Medicaid and Medicare.

In short, states need the power of advanced analytics to detect FWA and demonstrate where managed care plans have been ineffective at fighting it. Without that information, states have no leverage to question the managed care plans' total cost of care or to limit capitation payment growth. Health care costs continue to outpace inflation, and Medicaid costs comprise a significant portion of most state budgets, often the single largest cost to taxpayers. States need the tools to limit FWA and cost growth.

Organized crime rings have attacked many government COVID relief programs – how about health care?

Tom: Very much so. Organized crime has continued to migrate away from financial services and banking, where controls and technology have greatly improved, and toward health care. With U.S. national health care costs hovering around $4 trillion, health care is now a primary target. Identity theft has also become a big problem for health care systems like Medicaid and Medicare, at levels states haven't had to deal with in the past. A new threat, synthetic identity fraud goes beyond stealing a real person's identity to creating fake identities. Many states we have spoken with were unaware of this growing risk. We need to remember that the bad guys work on these schemes 24/7, and the money is so big that they're not going to slow down.

John: States need to improve their technology to understand the impact of the numerous data breaches occurring in health care, breaches that lead to identity

theft and fraud. Organized crime rings run national call centers using social engineering techniques and offers of free health care supplies to obtain patient medical billing data. This information is immediately used to bill for fraudulent health care claims. One federal investigation dubbed "Operation Brace Yourself" saw Medicare fraud of over $1 billion related to durable medical equipment alone. When dual-eligible patients are involved, part of the cost hits Medicaid.

As a former Payment Integrity Director, it drove me crazy knowing that we couldn't monitor all provider types all the time. Some fraud schemes are blatant. If a new provider joins a Medicaid network and immediately has claims skyrocket, it's like a thief throwing a brick through the front of a jewelry store. This type of smash-and-grab fraud sets off alarms. But other fraud schemes are hard to detect, and primitive rules-based approaches are ineffective. Smarter fraudsters steal smaller amounts using numerous schemes, what I call the "slow bleed" approach. It kept me up at night knowing these fraudsters were stealing our tax dollars. Even worse, organized health care fraud is often perpetrated by collusive provider and patient rings. Without the right technology, it's hard to spot these relationships.

This kind of fraud also means poor patient safety and health outcomes. Whether part of an organized ring or not, no fraudulent provider delivers quality care.

What technologies are we talking about, and how can they help?

Tom: Advanced analytics using artificial intelligence (AI), machine learning (ML), and a powerful analytics platform is key. In the past, most health care fraud analysts would manually run a single model or query focused on a particular provider or service type, then move onto another one. The problem with this approach is that cycling through all provider and service types could take three or four years. The limitations were large data volumes requiring significant compute power. Data had to be sliced and analyzed in small bundles, pieced together, and summarized. Such a lengthy and fragmented cycle left some provider types to go unmonitored and allows unnoticed overpayments and fraud to grow quickly.

Using AI and ML, advanced analytics can be run against all provider types at the same time, which helps expose fraud and minimize overpayments.

However, the technology has changed dramatically, especially with cloud-enabled services for handling big data. Today, automated analytics can scan health care claims rapidly and cost effectively, allowing for a broad and holistic view across providers and services that can uncover fraud earlier and more accurately.

John: Automating these manual processes is a game changer. As states and commercial payers struggle to find enough skilled data analysts and data scientists, automation promotes efficiency and better manages risk. Using AI and ML, advanced analytics can be run against all provider types at the same time, which helps expose fraud and minimize overpayments. Every time we talk to these data analysts, they consistently say that manual processing means other work is not getting done – like discovering new fraud schemes or exploring the FWA effects of policy changes. These analysts also report struggling with effectively managing advanced analytics models. However, a platform optimized for advanced analytics also means better model operations capabilities, especially for incorporating open-source languages and models.

The increased use of AI and ML for health care fraud detection enables more predictive analytics and better link analysis. Rules-based analytics are simply not as effective. In fact, the onset of COVID drove quick and significant changes to rules such as place of service, scope of practice, and use of telehealth, which rendered many rules-based models nearly useless. That opened the door to new COVID fraud schemes, but we also saw traditional fraud schemes resurface and grow quickly.

In contrast, an advanced predictive analytics approach that reviews all provider types can adjust to changes, filter the noise in the system, and spot new and emerging fraud patterns and links. We could see, for example, which providers were shifting to telehealth and how quickly, as well as changes in provider billing patterns. That kind of capability requires a holistic and hybrid analytics approach combining rules, anomaly detection, predictive models, and link analysis.

Tom: We talked about fraud rings, and that is exactly what link analysis spots so well. Using automation to identify collusive provider networks saves significant time, and using AI and ML to spot hard-to-detect patterns in the tremendously large data sets makes all the difference. Now we can see the connections between providers, the frequency and strength of the connections, and – using geo-mapping with link analysis – see and understand the locations of and distance between these providers.

Data visualization is also key. Adoption of analytics has been a struggle for many in the SIU. Whether their background is nursing, law enforcement, or other forms of investigation, they can find spreadsheets filled with statistics challenging. Today's data visualization methods can make sophisticated analytical information accessible to all staff.

Connected data can be at their fingertips without having to plow through multiple databases or systems. For example, color-coded graphics that visually depict provider risk make fraud easier to spot and help staff triage alerts and manage work processes more efficiently.

Keep in mind, however, that being able to see what your data "is" does not replace knowing what your data "means." Analytic solutions must have the capability to help you understand as well as visualize.

Where do you see this type of fraud-fighting technology going in the future?

John: It is a reality that health care lags other industries, especially financial services, when it comes to rigorous fraud and waste detection. But the road is being paved now to correct that, especially as the COVID-19 pandemic is accelerating the digital transformation of health care. Providers of all kinds and patients of all generations are transitioning rapidly to more technology-based ways of delivering and consuming health services. The future of health care will see the continued integration of technology like AI, internet-of-things devices, telehealth communications, and wearables – along with evolving payment models like value-based care and delivery models like whole person care.

That's health care technology itself. But what about the future of technology to fight health care fraud? It will be more focused on data security, cloud deployment, and real-time analytics of streaming data. FWA solutions must align to these broader strategic industry shifts; coordinate with related enterprise analytics solutions; and augment staff capability and efficiency with tools like computer vision, document vision, robotic process automation, and intelligent decisioning.

How does fighting health care FWA relate to health outcomes and equity?

Tom: The connections are more important than many people recognize. The linkage starts with the financial bottom line: when you stop or even prevent fraud, you have more money to spend on the people who need and truly benefit from the health services. You have better patient outcomes.

John: Health equity is generally viewed through the service delivery lens. Do people have equitable access to care and quality of care? Looking through a FWA lens, I believe that all patients deserve quality care, and that fraudulent providers will not offer it. In fact, they can put patients directly at risk of harm by performing unnecessary procedures. As an extreme example, doctors administer expensive chemotherapy after convincing healthy patients that they have cancer. SIU staff members, especially those who are former clinical practitioners, are becoming more aware of this close connection between FWA and patient safety.

Tom: Fraudulently billing for services not provided is also a problem from a health equity perspective. Home and Community Based Services (HCBS) are a prime fraud target because these services, like home health aides and transportation, require little training and have easy certification requirements. CMS identifies them as high-risk for fraud, yet care coordinators often assume that services are delivered as billed, and their relatively low-cost doesn't draw scrutiny. However, patients who need such services but don't get them may then require more high-cost hospitalizations or skilled nursing facility stays. Lack of basic HCBS can lead to falls, lack of nutrition, and other outcomes that harm patients. Additionally, fraudsters target the most vulnerable patients who are low-income, on disability, or suffering from depression or addiction.[2]

For health outcomes and equity, all patients deserve equal protection from FWA, but that can't happen if we're not pursuing fraud vigorously in programs like HCBS.

John: Sometimes states have trouble recruiting HCBS providers, and they assume that rigorous monitoring will scare off providers. In reality, this assumption attracts bad providers who feel they can operate with impunity. HCBS are often offered to elderly and disabled patients in Medicaid under CMS waivers. These patients desperately need these services to remain in the community and out of institutional care, but they are also desirable targets for fraudsters because they are less likely to advocate for themselves. Thus, fraudsters prey on these vulnerable populations.

I agree that not pursuing FWA across all programs and provider types puts certain patients at higher risk of harm and poor health outcomes. I'd even argue that this introduces an unacceptable form of bias into health care delivery. There's a lot of attention these days to recognizing and avoiding bias in analytical models and data sets. But there can also be bias in where we choose to focus the capabilities of analytics to begin with. States must never let program concerns lead them to inadvertently ignore fraud and create a bias that compromises patient safety. The CMS focus on fighting FWA in state waiver programs speaks directly to this need to ensure patients are safe and well-served, especially those at highest risk such as the disabled and senior citizens.

[2] https://www.justice.gov/usao-ma/pr/two-women-indicted-charges-stemming-100-million-home-health-care-fraud-and-money

John Maynard

Principal Industry Advisor, SAS

John Maynard is a subject matter expert in health care and government, part of the SAS Global Fraud & Security Intelligence practice. John is the former Program Integrity Director for Ohio Medicaid, the 5th largest state Medicaid agency in the U.S. with 3 million covered lives and now $29B budget. During his tenure there, Ohio was a national leader in health care fraud indictments and convictions. The collaborative efforts of Ohio Medicaid with the Ohio Auditor of State and the Ohio Attorney General's Medicaid Fraud Control Unit (MFCU) earned this group honors from the Harvard University's Ash Center for Democratic Governance and Innovation.

John has a BA in Accounting, and he is a Certified Public Accountant (CPA), Certified Fraud Examiner (CFE), and Accredited Healthcare Fraud Investigator (AHFI). John has spoken at state and national training conferences and taught at the national CMS Medicaid Integrity Institute. He is a former retail pharmacy technician and began his government health care career at the Ohio State University Wexner Medical Center and James Cancer Hospital Solove Research Institute.

Tom Wriggins

PRINCIPAL INDUSTRY ADVISOR, SAS

Tom Wriggins, with over 30 years of health care experience, is considered a thought leader within the government health care and data space. Calling upon his practitioner-level clinical knowledge and experience, Tom is responsible for business analysis and design, analytic design, data management consultation, application, and interpretation of comprehensive Program/Payment Integrity and Data Analysis Solutions.

Tom has shared his knowledge during conventions and conferences and has been the invited speaker for several industry association meetings. Tom served on the Division of Transplantation – OSP/HRSA/HHS Peer Review Panel for over 13 years as well as the HRSA HIV/AIDS Bureau – Special Projects of National Significance (SPNS) Program Data Collection and Management Peer Review Panel.

Prior to joining SAS, Tom spent over 10 years as the Practice Leader for one of the world's largest technology companies leading multidisciplinary teams that delivered large and complex data solutions for government health care entities, as well as creating training programs associated with fraud and abuse investigative solutions.

Tom holds a Bachelor of Science degree in Health Policy and Administration from The Pennsylvania State University. Tom resides with his family in Southwest Florida and Midcoast Maine.

Robert Morison

Robert Morison serves as a senior advisor for IIA. An accomplished business researcher, writer, discussion leader, and management consultant, he has been leading breakthrough research at the intersection of business, technology, and human asset management for more than 25 years. He is co-author of *Analytics at Work: Smarter Decisions, Better Results* (Harvard Business Press, 2010), *Workforce Crisis: How to Beat the Coming Shortage of Skills and Talent* (Harvard Business Press, 2006), and three Harvard Business Review articles, one of which received a McKinsey Award as best article of 2004. He holds an A.B. from Dartmouth College and an M.A. from Boston University.

IIANALYTICS.COM