dun & bradstreet

From Chase to Prevention

Stopping Healthcare Fraud Before it Happens

Healthcare fraud, waste, and abuse cost taxpayers tens of billions of dollars per year, with Medicare and Medicaid fraud alone estimated to cost $160 billion annually.[1] While state and federal agencies have historically been unsuccessful in controlling the growth of healthcare fraud, the program integrity provisions of the Affordable Care Act and the Small Business Jobs Act of 2010 have driven these agencies to aggressively seek solutions to combat abuse.

While chasing fraudulent payments after the fact has been standard practice, the Centers for Medicare & Medicaid Services (CMS) and forward-thinking state agencies are adopting new technologies and practices that allow them to prevent fraud before it happens by proactively identifying high-risk providers and suspicious claims. Methods such as data mining, predictive analytics, fraud scoring, and standardized provider registration – enabled by clean sets of in-house and third-party data – are allowing these agencies to target the highest-risk providers for investigation. Ultimately, these practices will help public and private payers to identify the main sources of abuse, prevent fraud, and cut costs.

UNDERSTANDING CURRENT TRENDS IN ABUSE

Unnecessary procedures are a common fraudulent activity, however submitting claims for services not performed is even more prevalent. A variation of that practice is upcoding – using billing codes for procedures that are more costly than the actual treatment.

Specific types of services also appear more susceptible to fraud than others. From a Provider Fraud Pattern analysis Dun & Bradstreet, a global provider of business insight and risk management solutions, has conducted from 2012-2014, the most chronic areas for abuse are ambulatory services, durable medical equipment, and home health services. These large markets, which comprise thousands of small-size providers and high volumes of daily transactions, make oversight difficult and their work hard to validate. The nature of their work is transactional and often subjective, and the difficulty of understanding what counts as billable work creates great potential for abuse.

Because of "creative" billing practices, healthcare costs are rising while access is decreasing for eligible beneficiaries. "There's an ongoing evolution of not only the methodologies fraudsters employ, but an incredible ability to exploit vulnerabilities unique to subcategories of providers," said Sandy Wright, Dun & Bradstreet director of business development. The more money these providers siphon from the healthcare system for purposes other than providing care, the greater the costs will be for taxpayers and healthcare recipients.

Fortunately, public and private payers alike can curb abuses and keep costs down by standardizing provider registration processes, verifying provider information with third-party data, and tracking the relationships between businesses and individuals. Through its extensive work with agencies,

Dun & Bradstreet developed three best practices to proactively address healthcare fraud.

Healthcare is a tempting target for thieves. Medicaid doles out $415 billion a year. Medicare spends nearly $600 billion. Total healthcare spending in America is $2.7 trillion or 17% of GDP. Fraud (and the rules and inspections to combat it) add as much as $98 billion or roughly 10% to Medicaid and Medicare spending – and up to $272 billion across the entire health system.[2]

1. CNBC: Medicaid Fraud Costs Taxpayers $160 Billion/Year. Accessed at http://video.cnbc.com/gallery/?video=3000103492
2. The Economist http://www.economist.com/news/united-states/21603078-why-thieves-love-americas-health-care-system-272-billion-swindle

BEST PRACTICE 1: DEPLOYING STANDARDIZED REGISTRATION PROCESSES

The creation of a standardized, rigorous registration process for Medicare and Medicaid providers is one of the greatest opportunities for fraud prevention. CMS has implemented the Automated Provider Screening (APS) system in an effort to identify high-risk providers; meanwhile, each state has its own system for onboarding. "This online registration creates an opportunity for 'bad actors' to get into the system, and once someone's in the system there is an implied assumption of validity," said Mark Muckerman, director of State and Local government solutions at Dun & Bradstreet. Inconsistent and insufficient data entry requirements have allowed large numbers of high-risk providers to successfully register, including providers who were excluded for fraudulent billing in other states.

Some states attempt to curb abuse with required updates, but the time lag between updates can hinder efforts to identify changes in the operating condition, ownership, or billing patterns of providers, which increases fraud exposure and puts beneficiaries at risk. A provider might obtain a National Provider Identifier (NPI) number, for instance, bill for falsified services, and move or change ownership several times before its home state requires an update on its activities and whereabouts.

Standardizing and automating online registration can address these problems by enabling complete assessment of provider risk upfront. "It's a lot easier to catch and identify high-risk providers on the front end than on the back end when you're tasked with mining mountains of claims data to look for the proverbial needle in the haystack," said Wright. To improve the quality and reliability of nationwide registration data, Dun & Bradstreet recommends provider verification across multiple jurisdictions, continual monitoring of good standing, and consistent input requirements among CMS and the states to support modeling, fraud scoring, and risk analysis. Ensuring accurate, standardized, and timely provider data during the provider registration process not only exposes would-be defrauders before they bill, but it also allows payers to use the resulting insights when applying predictive analytics to flag suspicious healthcare claims.

The five states with the highest number of fraud cases include California, Texas, New York, Ohio and Kentucky.[3]

BEST PRACTICE 2: VERIFYING PROVIDER INFORMATION WITH THIRD-PARTY DATA

No matter how rigorous, registration processes cannot provide all the information required by analytics to flag high-risk providers. One of the most common challenges Dun & Bradstreet sees with the available data is little to no external enhancement of provider profiles. The lack of third-party data curtails payers' abilities to verify and obtain insight into providers' self-reported information. Fraudulent providers often report existing addresses, for instance, but without third-party data enrichment, payers will not uncover – at least in a timely manner – the fact that those addresses belong to restaurants, hotels, or other non-medical businesses.

3. Health Research Funding http://healthresearchfunding.org/stunning-medicaid-fraud-statistics/

Checks of databases such as the Social Security Administration (SSA) Death Master File and the List of Excluded Parties and Individuals (LEIE) maintained by the Department of Health and Human Services' Office of the Inspector General, in addition to state medical license information, can help to identify risky providers. However, Dun & Bradstreet's analysis of provider files often reveals "red flags" in other areas such as a provider's operations and financial condition. This insight, when used in combination with the aforementioned sources, can significantly enhance the effectiveness of screening procedures by presenting a more comprehensive risk profile, while also identifying high-risk providers that would otherwise have gone undetected.

To obtain a complete view of potentially fraudulent behavior, payers should constantly update old business information and monitor providers for location changes, employment of unlicensed practitioners, and other potential signs of abuse. Adding business information provided by objective third parties fills in the gaps inherent in the usual data sets that payers aggregate. Relying solely on providers' self-reported information exposes agencies to outdated data and risk of fraud. Additional data either corroborates what businesses provide or flags their self-reported information for review.

Third-party data sources include Dun & Bradstreet's Healthcare Provider Risk Index, a proprietary risk-scoring system that evaluates and ranks providers' relative potentials to demonstrate characteristics consistent with known instances of fraud, waste, and abuse. By partnering with third parties to obtain additional data, payers can focus their limited resources on their main objective: to help provide needed services to eligible beneficiaries. Applying analytics solutions to complete data sets allows both public and private payers to "reduce the haystack" by efficiently narrowing provider databases to the small percentage who demonstrate the greatest potential for fraud, waste, and abuse.

Finally, while government agencies can share information with one another in an attempt to reduce fraud – although privacy laws prevent insurance companies from sharing certain claims- and payment-related data – even private payers are beginning to share information to identify fraud schemes and build complete sets of provider information. "Sharing information and using external databases are not unique to the public sector, and there are some forward-thinking people in the private sector who realize their benefits," said Muckerman.

> "People commit fraud, and knowing their relationships to each other and to healthcare businesses allows you to understand who might be involved in any given scheme and when and where it's likely to take place."

BEST PRACTICE 3: TRACKING BUSINESS AND INDIVIDUAL RELATIONSHIPS

In addition to monitoring provider organizations, understanding the relationships between individuals and business entities is critical for fraud prevention. Without a complete view of doctors, patients, and their relationships to clinics, hospitals, and health systems, payers face gaps in their abilities to analyze their data and understand where fraud might occur.

Recognizing suspicious persons and entities such as shell companies, physicians, and practices that move from state to state and patients who patronize out-of-town drug stores can make a dramatic difference in detecting abuse. “People commit fraud, and knowing their relationships to each other and to healthcare businesses allows you to understand who might be involved in any given scheme and when and where it’s likely to take place,” said Wright. By understanding these connections, payers might find that several providers, small practices, and beneficiaries are all working together to receive undue payments and discounted care, even across state lines. This insight can help federal and state officials prioritize investigations by focusing on those cases offering the greatest potential return on investment of resources. As with other information, understanding these relationships is a matter of combining the public sector’s best practices for analytics and predictive modeling with third-party patient and provider data.

PUBLIC SECTOR BEST PRACTICES PROVIDE A ROADMAP FOR PRIVATE SECTOR BEST PRACTICES

Ultimately, neither new technology nor process improvements alone can prevent healthcare abuse, and truly effective approaches marry technology with robust claims data, provider data, and external data. These combined components will only become more important as the number of people purchasing insurance through healthcare insurance exchanges increases. The current pay-and-chase system does not work, and the practices public agencies are adopting must be leveraged in order for the private sector to keep costs under control. “If the whole system, public and private, can be flipped to a preventative model, everybody wins,” said Muckerman.

Relying solely on providers’ self-reported information exposes agencies to outdated data and risk of fraud.