Decide with Confidence

Medicaid Fraud Prevention & Detection

Best practices for combating fraud, waste, and abuse

Executive Summary

Medicaid fraud, waste and abuse cost taxpayers up to $160 billion annually[1]. This problem deprives eligible beneficiaries of needed services and puts their health at risk, exposing them to sub-standard services. While Medicaid is one of the largest, fastest-growing line items in most state budgets, state and federal efforts to prevent and detect healthcare fraud have been challenging. The growth in Medicaid expenses, coupled with the program integrity provisions of the 2010 Patient Protection and Affordable Care Act, have led states to adopt a more aggressive stance to combat fraud, waste and abuse. As part of this effort, states are increasingly looking to employ best practices from the commercial marketplace such as predictive modeling, provider screening and data mining and analysis to uncover fraud schemes perpetuated against state Medicaid programs. Despite the differences in these approaches and the phase of the healthcare delivery and billing process in which they are deployed (e.g. initial eligibility determination, claims review), they all require access to accurate, current and complete information on providers and beneficiaries.

> *"National Medicaid data are not current, they are not complete and they are not accurate. In fact, the National Medicaid data does not capture all of the elements necessary for the detection of fraud, waste & abuse. Missing data includes elements as basic as name, address and billing information"*[2]
>
> **Ann Maxwell**
> Regional Inspector General
> Office of Evaluation and Inspections
> Office of Inspector General
> Department of Health and Human Services

As the world's leading provider of commercial insight for over 170 years, Dun & Bradstreet (D&B) is uniquely qualified to help states overcome common data-related challenges that undermine program integrity initiatives, including duplicate records, outdated or inaccurate address information, limited visibility into connections between providers and beneficiaries, and the inability to accurately assess the risk associated with businesses and individuals.

D&B's Medicaid Fraud Prevention and Detection Services offer a cost-effective, data-driven approach to combat Medicaid waste, fraud and abuse. D&B can help you identify unique providers and beneficiaries, "cleanse" existing records by accessing more current and accurate address information and "reduce the haystack" by identifying "red flags" or risk factors that reflect potentially fraudulent or high-risk behavior.

D&B's Medicaid fraud prevention key capabilities
Mature database of over 600 million individuals (including deceased) and businesses to authenticate and screen providers
Use of industry-proven matching algorithms and global identification standards to uniquely identify individual providers and integrate disparate sources of claims and payment data
Robust investigative and monitoring capabilities to facilitate additional due diligence on new and high-risk providers and alert states to critical events (e.g., bankruptcy filing) occurring after enrollment
170+ years of experience in supporting risk identification, assessment and management needs of both public and private sector organizations

[1] http://video.cnbc.com/gallery/?video=3000103492

[2] Testimony on June 14, 2012 - Subcommittee on Federal Financial Management ,Homeland Security and Governmental Affairs

More specifically, D&B’s Medicaid Fraud Prevention & Detection Services will help you to:

- Correct the addresses of Medicaid Providers, thereby ensuring they receive important correspondence and communication. D&B’s previous analysis of state provider files has revealed that between 17%– 30% of records have outdated or inaccurate addresses.
- Accurately link related providers through D&B Corporate Linkage, giving you the ability to understand connections between providers (and beneficiaries) and assess total risk exposure.
- Verify the existence and legitimacy of providers by leveraging D&B data assets such as business registrations, type of address and payment experiences (or lack thereof).
- Use D&B predictive risk scores such as our Financial Stress Score (FSS), which predicts the likelihood of business failure over the next 12 – 18 months, for quick, “at-a-glance” insights into the financial and operational stability of both Medicaid program applicants and current providers.
- Proactively identify and focus investigative resources on those providers most likely to be engaged in “fraud-like” behavior.
- Create a risk profile based on “known bads” (e.g. providers previously flagged for Medicaid fraud) and use this profile to screen current and prospective providers

Overall, third-party D&B intelligence combined with Medicaid and other agency operational data and data mining and analytical tools will provide your state with improved insight to detect fraudulent patterns and predict behaviors more effectively. This is accomplished through our Data Optimization and Enrichment Services, including D&B’s best practice approach to standardizing, cleansing, enriching and transforming provider and beneficiary data into actionable intelligence.

> “The Texas experience is that ***more data is better***. Whether the data comes from ***Medicaid, Medicare, SNAP, WIC, TANF, Craig’s List, county property lists, banking records, arrest records, employment records or nearly any other source you can imagine***, all of this data can help to identify patterns of behavior and billing which lead to identifying intentional or inadvertent overbilling and the accompanying overpayment.”[3]
>
> **Douglas Wilson**
> Inspector General, Health and Human Services Commission, State of Texas

Data Optimization and Enrichment Services

By leveraging D&B’s Data Optimization and Enrichment Services, your state will receive complete and current information about providers and beneficiaries to further enhance your own data mining, predictive modeling and analysis initiatives. We accomplish this by using a sophisticated set of patented matching algorithms, linking technologies and information standards, such as the D-U-N-S® Number, the global company identification standard, and our referential database, which contains billions of potential match opportunities for provider records.

[3] Testimony on June 14, 2012 - Subcommittee on Federal Financial Management ,Homeland Security and Governmental Affairs

Our solution includes the following steps:

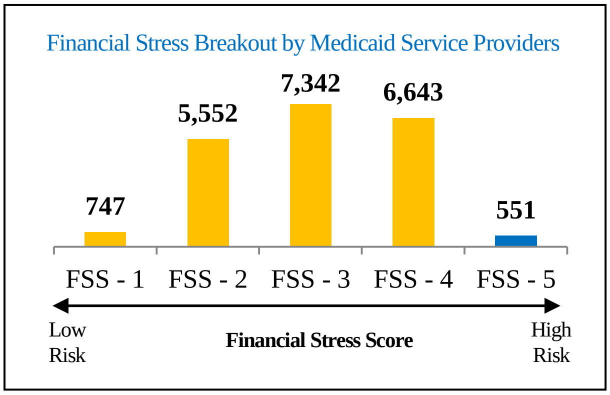
- Cleansing employs our best-in-class, patented processes to correct address inaccuracies, format inconsistencies and standardize name and address information.
- Identification (matching) assigns a D-U-N-S® Number to business entities and establishes a link to the up to 1,000 different data elements associated with each record. Distinct locations are also identified, as well as linking individual practitioners (providers) to a practice or multiple practices.
- Enrichment includes appending enhanced information to your provider records:

Employee Counts and Annual Revenue	Debarment Status
Industry Classifications (SIC/NAICS Codes)	Payment Experiences
D&B's Financial Stress Score	Corporate Linkage & Affiliated Practicioners
Out of Business / Bankruptcy Indicator	High Risk Address Sweep
Criminal Activity Indicator	Unconfirmed Operations Indicator

Results in Other States

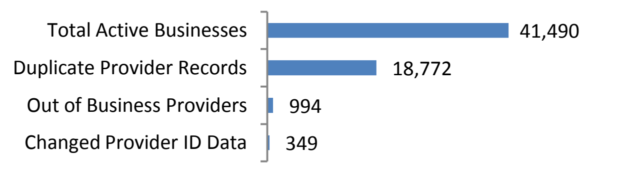
D&B's engagement model for our Medicaid Fraud Prevention & Detection Services includes the analysis of provider and beneficiary files to assess file integrity and identify the risk within each portfolio. States that have taken advantage of this solution have found it helpful to understand how clean their data is and their amount of risk exposure. Typically, once D&B receives your provider file, we will provide you with the following analysis:

- Full Matching Analysis
  - How well did your file match to our Provider Database?
  - How many records did our cleansing process correct on your file?
  - How many records from your file are "Out of Business" or whose operations we were unable to confirm?
  - How many duplicate records are you maintaining? (We typically see duplication rates of up to 50%)
- Uncover linkages between doctors to practices
- Financial Stress Profile – indicating companies likely to go out of business
- Providers featuring "red flags" (e.g., criminal indictment, debarment, bankruptcy)
- Providers located at "high-risk" addresses (e.g., residences, nightclubs, restaurants, storage facilities)
- Addresses and Social Security Numbers associated with fraudulent behavior

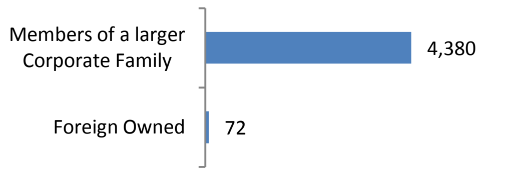


Sample Analysis

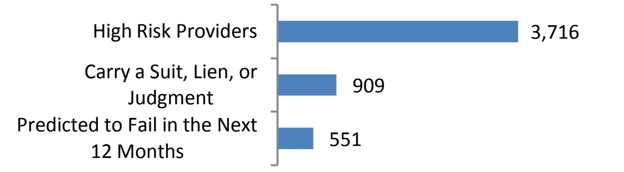
File Profile



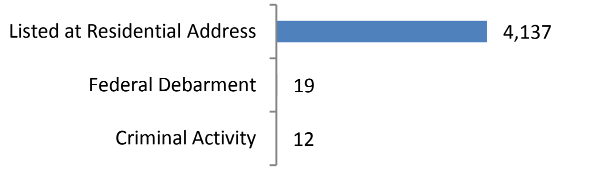
Business Profile



Financial Risk Profile



Red Flags



Address Analysis highlight areas of potential fraud

Reason	County #1	County #2	County #3
Input address is a campsite	1	4	2
Input address is a check cashing service	0	4	1
Input address is a correctional institution	7	14	3
Input address is a credit correction service	2	7	1
Input address is a hospital or clinic	6	70	16
Input address is a hotel or temporary residence	7	5	2
Input address is a mail receiving/forwarding service	18	9	0
Input address is a multi-unit reported misuse	28	51	21
Input address is a multi-unit reported suspicious	0	1	0
Input address is a nursing home	158	667	315
Input address is a restaurant/bar/night club	8	33	21
Input address is a secretarial service	0	0	0
Input address is a storage facility	1	6	5
input address is a truck stop	0	1	0
Input address is a U.S. Post Office	0	3	2
Input address is commercial	0	0	0
Input address is commercial	0	0	0
Input address in governmental	1	4	4
Input address is institutional	0	0	0

Reason	County #1	County #2	County #3
Input address reported as suspicious	21	50	8
Input address reported misused	114	231	30
Input address requires further investigation	6	5	0
Input address used in true name fraud or credit	58	224	17

Prioritize for further investigation

Risk categories of interest

Requires Further Investigation: The address matches an address on the High Risk file, but no further information was provided.

True name fraud: The address matches an address identified as used in a true name or credit fraud.

Suspicious: The address matches an address on the High Risk file that could not be verified when it was used on previous inquiries.

Misused: The address matches an address on the High Risk file reported used in a potential or known fraud.

This analysis allows agencies to be proactive in their fraud mitigation efforts, by helping you find the "needle in the haystack," - the 1-5% of providers with the potential to be engaged in Medicaid fraud. States can seize the advantage against fraudsters by taking a proactive approach to combating fraud, waste, and abuse by Medicaid providers and recipients. D&B's Medicaid Fraud Prevention and Detection Services offer a cost-effective, data-drive approach that will provide states with improved insight, allowing them to detect fraudulent patterns and predict behavior more effectively.

Brent Mears Director of Business Development, U.S. West 512.651.5188 mearsb@dnb.com