IBM Fraud Intelligence Solutions for the social sector
September 2007

A proactive approach to Medicaid fraud, abuse and error detection

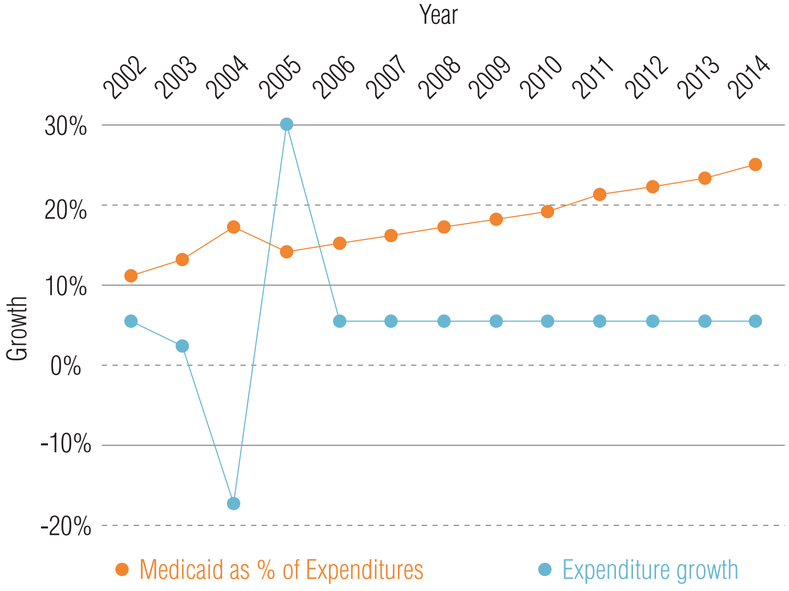
IBM Fraud Intelligence Solutions

by Bryan Chong, Juan Penalosa and David Dyda

Introduction

In recent years, Medicaid expenditures have become one of the most expensive line items on state budgets. Accounting for more than 15-20 percent of budgets, the amount states annually expend on Medicaid benefits can easily surpass expenditures for Public Safety and Transportation.*

Projected growth of Medicaid as % of total expenditures



With a significant amount of the budget at stake, states are under more pressure than ever to identify fraud, abuse and error to ensure program dollars end up in the right hands. However, traditional passive detection methods typically detect inaccuracies only after the fact, when benefits have already been paid to the wrong people. States today need a more active, preventive approach to fraud, abuse and error detection – ideally, one that is capable of integrating with case and risk management applications to help ensure the right eligibility decisions are made before benefits are extended.

This white paper describes the challenges and trends facing Medicaid organizations, including traditional approaches used to determine eligibility requirements and various forms of improper benefits payment occurrences. The paper then discusses how IBM Fraud Intelligence Solutions (FIS) offers a proactive approach to help reduce fraud, abuse and error. Initially created to aid law enforcement, the intelligence community and money laundering investigations, IBM FIS can help Medicaid agencies better identify rings, ineligible recipients and providers, and unmask fraudulent identities and relationships.

Specifically, the paper will describe how IBM FIS can help Medicaid organizations:

- *Gain a comprehensive and self-improving view of identity and fraud information that utilizes multiple sources of information within and beyond the organization.*
- *Move to a more active and dynamic approach, where the system can help verify recipient identity and uncover hidden or non-obvious relationships between applicants and other benefit recipients.*
- *Transform from an ex-post facto system of analysis and reporting fraud, eligible recipients and providers to the ability to access information in-line and on demand, e.g., to quickly determine if a recipient is applying for the same benefits in more than one jurisdiction.*
- *Compare recipient eligibility information across programs and jurisdictions anonymously in order to comply with privacy legislation.*

Medicaid challenges and trends in managing identity and eligibility

Medicaid organizations are frequently confronted with significant amounts of ambiguous and unvalidated data regarding the identity of their recipients and providers. This ambiguous data may be due to deliberate attempts by recipients or providers to obtain payments or just simply the result of an unintentional error. Even a seemingly negligible number – e.g., 1 percent – of duplicate and ineligible recipients can have a significant impact: In a state that plans to enroll 1 million people into managed care programs, this can translate to tens of millions of dollars in inappropriate spending.

But as states have attempted to validate and eliminate ambiguous recipients from their rolls, they have found themselves struggling to identify duplicate Medicaid recipients, recipients who are deceased and recipients who no longer qualify for Medicaid, but remain on the rolls. In many cases, the cause can be traced to inflexible, outdated technologies.

At the core of these Medicaid systems, a citizen database repository typically contains identity attribute information such as name, address, social security number and other vital information. Often, however, multiple databases residing in other departments maintain different versions of the data about a recipient or provider. Separate databases may exist for specific programs such as disability, child allowance and employment insurance. These different databases are rarely integrated, resulting in silos that contain conflicting and out-of-date identity information.

For example, when a recipient passes away, local governments provide death data to the state government to update the identity repository where it is then shared with other social services benefit programs. Due to stand-alone systems, inadequate data matching routines and privacy legislation, this update is prone to error and often a major cause of data integrity problems.

And while many state and federal government agencies share recipient identity data freely, Medicaid organizations require strict privacy protection and data security measures. The challenge of sharing and storing recipient information with required agencies (Attorney General, etc.), jurisdictions and third parties, in a secure manner that meets stringent privacy protection statutes will continue to grow in the coming years.

Most states also use naïve identity matching, which is composed of a set of identity matching solutions including one or more of the following:

- ***Merge/purge.*** *Originally developed by direct marketing organizations to eliminate duplicate customer records in mailing lists, these systems generally operate on data in batches; when organizations need a new de-duplicated list, they must run the process from scratch.*
- ***Binary matching.*** *This system tests an identity in one data set for its presence in a second data set. These matching engines are also sometimes used to compare one identity with another single identity (versus a list of possibilities), with the output often expected to be a confidence value pertaining to the likelihood that the two identity records are the same.*
- ***Centralized identity.*** *These systems collect identity data from disparate and heterogeneous data sources and assemble it into unique identities, while retaining pointers to the original data source and record with the purpose of creating an index. Such systems help users locate enterprise content much in the same way a library's card catalog helps people locate books.*

The primary problem with the identity matching technologies currently used by states is that they are only capable of obvious identity matching and do not attempt to address identity resolution needs or non-obvious relationships. Those running the identity matching solutions must constantly update relationships (i.e. Bob = Rob = Robert), and the quality of the data matching is only as good as the set of rules provided to the matching technology.

In essence, they are capable of doing little more than matching one singular set of rules to another singular set of rules, thus limiting the types of identities and relationships that a Medicaid agency can uncover. The fact that most need to be rerun from scratch each time rules are changed is also a barrier because they are not run as often as recommended due to limited time and resources.

IBM Fraud Intelligence Solutions: An overview

Presenting an entirely new level of precision to identity resolution and relationship resolution. IBM FIS is a robust suite of technology solutions used by government, law enforcement agencies and private sector clients (e.g., insurance and banking) to provide real provider and recipient identity recognition. With the ability to examine the anomalies and inconsistencies in data, FIS can help organizations better eliminate the inappropriate Medicaid spending attributed to ambiguous provider and recipient identities in Medicaid rolls or those who are ineligible, but have not been identified as such due to inabilities to properly construct identity profiles.

Designed to provide governments with a more detailed capacity for identifying, resolving and uncovering identities, FIS provides an automated resolution capability that operates in real time across both historic and current data to analyze identities and relationships of all accumulating data about recipients and providers. The resolution function is performed in the context of Medicaid processes to support proactive decision making.

FIS builds on its identity recognition capabilities to incorporate both non-obvious relationships and the facilitation of anonymous data sharing. FIS includes four Entity Analytics (EAS) components: Identity Resolution, Relationship Resolution, Anonymous Resolution, and Global Name Recognition.

- *IBM Identity Resolution is a technology that enables organizations to answer the question "Who is who?" Identity Resolution is able to distinguish whether multiple records are, in fact, records for a single resolved identity.*
- *IBM Relationship Resolution builds off resolved identities created by Identity Resolution. Relationship awareness provides answers to the question "Who knows who?" by seeking out non-obvious relationships between individuals and with organizations.*
- *IBM Anonymous Resolution allows several organizations to share and compare data in order to discover "Who is who and who knows who …anonymously?" Anonymous resolution converts confidential information into cryptographic form enabling data owners to maintain control of what information is revealed and concealed.*
- *IBM Global Name Recognition provides advanced name matching analysis. Not only does it provide the ability to perform automated name processing with English-sounding names, but it has advanced multi-cultural name recognition products for international governments and commercial clients worldwide.*

The FIS solution pulls from any number of data sources to generate identity records. By allowing for a full range of identity data points to be compared simultaneously and in conjunction with one another, FIS allows for identity evaluation against fully pre-constructed identities. These identities are made up of the accumulated attributes of all prior records. This technique enables new records to match to known identities completely, rather than relying on binary matching that can only match records in pairs. This context accumulation improves accuracy and greatly improves the handling of low-fidelity data that might otherwise have been left as a large collection of unmatched orphan records.

The FIS solution supports actions triggered not by a single event, but by a complex composition of events, happening at different times, and within different contexts. As an example, large amounts of inappropriate Medicaid spending are often the result of patients who are incorrectly enrolled in a more expensive capitated care program (i.e., a child is enrolled in an adult managed care program for the disabled) due to failure to properly identify the enrollee. FIS to can help detect changes in data about recipients and providers on a continuous basis and create a unique identity identifier that enables states to address the issue of inappropriate enrollment. Because the identity profiles are stored, FIS can be used to scan enrollees of specific programs and it will quickly identify those that do not belong. In addition, alerts can be generated as new information is added throughout the lifecycle of, and in line with, the Medicaid case management process. This enables the case worker to act on new information, so the opportunity is never lost to act.

For example, if new changes in the circumstances of a patient are detected (e.g., becomes disabled), FIS can provide an automated alert to the case worker and send the recipient into a queue for evaluation by a case worker. Or, FIS can use birth information located in a separate registry and department to provide an alert when a child turns a certain age so that a case worker could place the new adult into a more appropriate adult managed care program.

Another common scheme for perpetuating fraud and abuse in the managed care system is the result of relationships between providers who are using the complexity and relationship of the fee-for-service and managed care service to secure kickbacks. One such plan results when a fee-for-service provider and a managed care provider work together to refer patients to one another inappropriately and over time in order to garner the maximum amount of dollars from the Medicaid system, or when a provider who has been banned from the system re-registers under a different name or in conjunction with another provider to assist in defrauding the system.

In addition to uncovering fraudulent or erroneous enrollment in programs under the traditional fee-for-service model, FIS provides states with a powerful tool for managing costs in the Managed Care arena. Texas, Georgia and a number of other states have recently re-dedicated many of their Medicaid enrollees to Medicaid Managed Care (MMC) programs. Unlike fee-for-service programs, under MMC, third-party vendors manage the uncovering of fraud, waste and abuse on a provider level as the state pays the MMC a set amount per Medicaid enrollee. FIS is particularly useful in ensuring that states pay no more than is necessary. Recent proof of concepts have indicated that states have nearly 10-20% roll duplication. In other words, the same person appears on Medicaid rolls multiple times under slightly different names, either by accident or as a result of fraudulent behavior. In a MMC solution, the state would pay a set dollar amount for each of these duplicate enrollees. FIS can help states identify which enrollees are ambiguous or duplicates and ensure that they are not paying out funds unnecessarily.

FIS helps identify suspect activity by those with non-obvious or hidden relationships with multiple degrees of separation. This is possible because, unlike identity matching solutions, FIS produces an identity profile made up of many pieces of information which is stored in the system. Once an identity is created, FIS can begin to compare the identity profile and all relevant pieces of information with other identity profiles and all of their corresponding pieces of information now and in the future.

This comparison creates a very useful outcome from deployments of identity resolution in Medicaid agencies. The result could be the discovery of fraud that previously had not been considered. The original intention could have been to discover recipients of interest attempting to transact with the social services agency, but because the design placed all identities in the same data space, the good recipients, bad guys (subjects of interest), and providers co-mingled as they were matched against each other. This can result in new kinds of alerts—such as a physician who is at the nexus of several Medicaid cases of interest to the social services agency.

A powerful solution for verifying recipient application data, IBM FIS can help organizations take the first step toward proactive eligibility determination, before benefits and services are erroneously extended. Optionally, other IBM solution components provide complementary capabilities to build upon your existing technology investments:

- *IBM WebSphere® Customer Center provides a single view of recipients and providers.*
- *IBM Information Server helps organizations integrate disparate data.*

Why IBM?

Successfully addressing the challenges facing Medicaid organizations requires more than new technology; it requires a comprehensive approach, based on a clear understanding of the issues, a deep understanding of the business, advanced technology thinking and talented professionals who are passionate about what they do. As the largest provider of solutions for the social sector worldwide, IBM is able to bring together this powerful combination to help Medicaid organizations better prevent fraud, abuse and error.

In addition, IBM Global Social Segment has a dedicated team of subject matter experts, solution developers and industry consultants focused on Medicaid and social services organizations. IBM has invested in a portfolio of industry solutions and thought leadership to help organizations take advantage of global best practices in the social sector. Visit **ibm.com**/government/socialsegment for an online self-assessment of capabilities in this space.

As Medicaid agencies pursue initiatives to reduce fraud, abuse and waste, an important element to help ensure success may be to team with a partner to help develop a strategy, a business value assessment (BVA) and a business case.

IBM consultants plan and execute the BVA employing a proven assessment method to help Medicaid agencies gain the maximum benefits and insight into the organization. The BVA offering provides a set of tools to prioritize and analyze the impact of making an FIS Solution investment, or adding more function to an existing case and risk management system. Because the BVA is modular, Medicaid agencies have the flexibility to choose the modules that address their business needs. The BVA method can help:

- *Align the Medicaid organization and IT management with a common and prioritized set of identity disambiguation capabilities for case management and risk management system(s).*
- *Provide a visualization of the solution when it is complete.*
- *Provide a high-level cost and benefit analysis.*

For more information

To learn more about IBM Fraud Intelligence Solutions and the IBM Business Value Assessment, visit **ibm.com**/software/data/ips/solutions/risk-compliance/healthcare.html, or contact your IBM Software sales representative.

IBM Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
09-07

*National Association of State Budget Officers, "The Fiscal Survey of States," December 2006

Each IBM customer is responsible for ensuring its own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law.