

White Paper

Game-Changing Medicaid Fraud Prevention: How Data Mining Technology Empowers Medicaid Fraud Control Units (MFCUs) to Protect Program Integrity

October 2014

New legislation and new technology create new possibilities for MFCU program integrity protection.

Medicaid Fraud Control Units (MFCUs) have an important and difficult role—that of investigating and prosecuting Medicaid fraud. Until recently, due to a lack of access to data and technology, MFCUs have been limited in their ability to detect and mitigate fraud, and to protect the integrity of their State Medicaid programs. Understaffed, underfunded, and formerly forbidden from legally mining Medicaid data for fraud identification and prevention purposes, it has been an ongoing challenge for MFCUs to keep pace with complex and evolving fraud and abuse tactics. MFCU activities have been driven by back-end responses to referrals from Medicaid Program Integrity divisions, responding to Qui Tam cases or investigating tips from informers. MFCUs have historically been limited to addressing patient abuse ‘after the fact,’ only allowed to initiate investigations after patients were harmed or even killed.

Patient abuse²

- About one-quarter (350) of criminal convictions nationwide involved patient abuse and neglect. Cases of patient abuse and neglect included:
 - Aggravated assaults
 - Injury to elderly or disabled persons
 - Theft of patient funds

Two major changes have recently empowered MFCUs with new opportunities to detect, prevent, and mitigate fraud and abuse through a proactive front-end approach that provides unprecedented effectiveness and efficiency. These changes are:

1. New legislation, which allows MFCUs to access Medicaid data in order to detect potential fraud.
2. New data-driven technologies and analytics that can detect and reveal indicators of Medicaid fraud and abuse by identifying patterns and anomalies in Medicaid claims and other public records data.

With legal access to relevant data and the automated tools to uncover the truth hidden in the data, MFCUs can now equip themselves to identify and prevent fraud and abuse more efficiently and effectively. The successful use of these tools has the potential to result in tens of millions of dollars in cost avoidance savings and recovery per state.

The MFCU's challenging circumstances

Fraud and abuse of health care services cost the U.S. \$125 to \$175 billion per year, with Medicare and Medicaid fraud and abuse costing taxpayers about \$98 billion per year.¹ Unfortunately, only 3-5% of health care related fraud, waste and abuse cases are actually detected.

With new rules come new opportunities

On May 17, 2013, the Health and Human Services Office of Inspector General (HHS OIG) created new Federal Regulations³ that gave MFCUs the green light to data mine Medicaid provider, recipient, and claims data for the purpose of detecting fraud, waste, and abuse in their programs. Data mining is the process of transforming raw data into useful information by cross-referencing and analyzing the data in a variety of ways. In this case, Medicaid data could be mined to look for connections and patterns that are proven to be indicative of fraud. The Centers for Medicare & Medicaid Services (CMS) stated that allowance of MFCU data mining was “enacted to strengthen the capability of the Government to detect, prosecute, and punish fraudulent activities under the Medicare and Medicaid programs.” It is now the responsibility of each MFCU to develop a plan and seek approval from the HHS OIG to accomplish this expanded fraud detection mission.

Thanks to the new regulatory allowances, MFCUs are empowered to use Federal matching funds to acquire data mining tools and analytics technology to improve their efforts in identifying and mitigating fraud across Medicaid programs.³

“A significant factor in the increased productivity and success of the Medicaid Fraud Control Unit has been the ... fraud detection system.”⁴

Getting started: How the process works

Before a MFCU can begin data mining for fraud and patient abuse indicators, it must proactively seek HHS OIG approval by completing and submitting an application. Instructions describing application content and submission, as well as examples of approved applications, can be found on the OIG HHS website.³

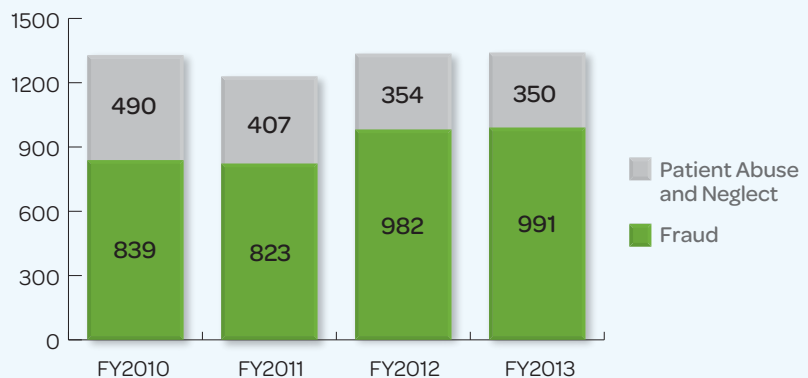
The following is a brief overview of the required application content:

- **Coordination Plan** – MFCUs must establish and explain how they will coordinate data mining activities with their State Medicaid Agency (SMA). The Coordination Plan must include:
 - Procedures describing coordination between the MFCU and SMA and rules in place to ensure duplication of effort is avoided
 - The primary points of contact for data mining at the MFCU and SMA
 - An amended memorandum of understanding between the MFCU and SMA
 - A description of the SMA’s level of support for the application to data mine
- **Staffing and Training Plan** – Each MFCU must assign and indicate the specific personnel that will perform data mining and describe the data mining training that each staff member will receive.

2013 criminal convictions²

- MFCUs reported 1,341 criminal convictions
- Criminal case recoveries reached nearly \$1 billion

Number of Criminal Convictions by Type of Case (Fraud vs. Patient Abuse and Neglect), FYs 2010–2013



Source: OIG analysis of Quarterly Statistical Reports, 2013

- **Reporting Plan** – Each MFCU must submit a plan to gather, monitor, and report on:
 - Annual expenses related to data mining activities
 - A record of the staff hours applied to data mining functions
 - The number of cases generated
 - The outcome and status of each case (including estimated and actual monetary recoveries)
 - All other potential indicators of data mining return on investment (ROI)
- **Budget Implications** – Each MFCU must indicate the estimated expense of implementing data mining operations, including staff time, equipment, and service costs.

Applications must be submitted electronically to both the director of the Medicaid Fraud Policy and Oversight Division and to the Unit's MFCUs assigned oversight program analyst. The HHS OIG will acknowledge receipt of the application and has 90 days from receipt to review a written request, consult with the CMS, and approve or deny the application. If the State OIG doesn't respond within 90 days, the application will be considered automatically approved.

Federal matching

The CMS HHS OIG will match state dollars with a subsidy of 75%. Therefore, each MFCU must secure state dollars—the amount secured will represent 25% of total program dollars. It is important that each MFCU develops its own data mining program plan in order to estimate the overall program costs and the budget required to create and sustain it. The strategic plan should include a budget that reflects short-term program upstart costs, long-term program growth and projected financial impact through increased cost avoidance and recoveries.

Currently, the HHS OIG administers grants that provide Federal funding for Unit operations based on 12 OIG-designated performance standards. Quarterly and annually, MFCUs provide the HHS OIG with investigation and prosecution performance and statistics, and other operational data. The HHS OIG analyzes these reports (along with other information) to determine MFCU recertification qualification. An effective data mining program can increase the likelihood of grant approval and recertification by substantially enhancing performance numbers in several relevant performance categories, including:

- **Maintaining a continuous case flow** – Analytics should reveal substantially more instances of potential fraud, creating a steady flow of case investigations.
- **Case mix** – Analytics should reveal a variety of fraud and patient abuse case types.

The CMS HHS OIG will match state dollars with a subsidy of 75%. Therefore, each MFCU must secure state dollars—the amount secured will represent 25% of total program dollars. It is important that each MFCU develops its own data mining program plan in order to estimate the overall program costs and the budget required to create and sustain it.

- **Maintaining case information** – The tools available today make it easy to manage, track, and archive case information.
- **Program recommendations** – New data mining programs should open the door for many innovative statutory, administrative, and operational recommendations.

2013 civil settlements and judgments²

- MFCUs reported 879 civil settlements *and judgments*
- Recoveries from civil cases totaled over \$1.5 billion
- 62% - Pharmaceutical manufacturing
- 6% - Pharmacies
- 5% - Home health care agencies

- **Fiscal control** – Advanced data mining technology includes scoring capabilities to prioritize cases based on the amount of evidence of fraud available, the scope of the case, and the likelihood of the recovery of funds. This translates into budget optimization and a higher return on each dollar invested.
- **Staffing** – Added efficiencies from automated technologies enable increased cost-avoidance savings without increased staffing.

To-date, five MFCUs have active data mining plans: Florida, California, Missouri, Oklahoma, and Michigan. MFCUs in other states may find value in requesting copies of the required reports (from MFCUs with active plans) for reference when completing their own state's application.

The Solution: Unleash the Power of Today's Cutting-Edge Technology

Key considerations for MFCU plan development

As you develop your new data-driven fraud prevention plan, be sure to consider the new capabilities available to you through the adoption of robust data mining tools and technologies. Advanced solutions are capable of seamlessly supplementing Medicaid-specific data with massive amounts of critical data from outside sources such as public records. The combination of these unique data sources brings significant value to an investigator. Subtle links and connections revealed in non-Medicaid data can provide a wide range of fraud indicators that would be undetectable when relying on traditional in-house means. For example, a specific provider may not have a criminal history of fraud, but may have direct relatives or business associates with prior Medicaid fraud convictions, resulting in a significantly higher risk of fraudulent activity.

Products and services that provide this critical context to existing Medicaid data can be easily accessed through secure online portals and are surprisingly affordable. Designed specifically for Medicaid Program Integrity, these solutions are significantly more streamlined and effective than traditional investigative methods and typically generate a very high return on investment (ROI). Further, these mediums enable investigative staff to detect, investigate, and conclude more cases by providing the means to work faster and more efficiently.

MFCUs can now detect, investigate, and prosecute billing fraud and waste, as well as address patient abuse, in powerful new ways. While the phrase "data mining" is typically used to describe the process of using Medicaid provider and recipient data to detect fraud, recent advances in health care fraud detection technology go far beyond simply combing through claims data. By combining Medicaid data with public records data (sometimes called "Big Data"), and leveraging highly-advanced data analytics, fraud detection capabilities have reached unprecedented levels of speed, efficiency, accuracy, and effectiveness. Here are some of the specific tactics that can be employed:

- Automatically validate Medicaid provider and recipient data against rules and guidelines set by the American Medical Association (AMA), the Correct Coding Initiative (CCI), and the CMS, including state-specific CMS rules.

- Leverage pattern recognition technology that looks for information that should and should not be present based on industry standards, impossible events, and flags indicating anomalies or suspicious patterns.
- Analyze patient, provider, and claims data with Big Data public records, which contain years of relevant data, to verify information such as: identity attributes, Social Security Numbers, criminal history, license exclusions, and other high-risk elements. Inconsistencies, or unverified data points, are flagged and can be further researched.
- Flag claims information associated with deceased and incarcerated providers—both strong fraud indicators.
- Reveal hidden connections and relationships with known or suspected fraudsters or patient abusers.
- Identify collusion (i.e. providers working from fake or storefront operations) using a combination of public records data and traditional provider, recipient, and claims data to run social network analyses.
- Allow non-technical users to easily run ad hoc queries and build suspect lists.
- Optimize resource allocation and improve overall program effectiveness by prioritizing and triaging case workload through the sophisticated scoring of claims and providers. Scores can be calculated based on a variety of factors, such as: level of confidence of fraud, type of suspected fraud, potential scope of the monetary impact, likelihood of recovery, and others.

“We now have instant access to electronic data. Tasks that in the past took weeks can now be done in minutes.”⁴

Innovative MFCU data mining solutions are capable of “mass analysis” of high volumes of claims data, including hundreds of millions of claims, providers and recipients, and provide MFCU staff with well-documented, easy-to-understand, and actionable analyses. Combined with a reliable rules-based fraud detection system, these solutions pinpoint suspicious behavior across all health care claim types, including medical, facility, pharmaceutical, mental, and dental claims. Instances of potential fraud are then presented as actionable information that is easy to understand, investigate, and pursue. Advanced predictive models actually adapt and evolve, becoming more intelligent as they learn from accumulated information and analytic output.

Some tools include options with drill-down capabilities that enable users to easily trace leads by provider, recipient, transaction, and other related data. Specialized screens assist investigators in identifying providers or claims based on partial information, or tips from fraud hotlines. The most versatile systems even provide functionality for non-investigative departments such as provider relations, medical directors, finance and audit, among others.

Success summary

One southwestern state’s Program Integrity (PI) Unit has been using advanced intelligent data mining technology for approximately five years with extraordinary results. Last year alone their PI Unit recovered more than \$52 million with recoveries being either directly or indirectly linked back to insights exposed through the data analytics.

"[The system] has changed the way this Unit investigates providers. It has provided more high-quality referrals and better support for those referrals. It has made the Unit more efficient and provided enormous savings in Unit resources. As a result, the MFCU has greatly increased its productivity in both criminal convictions and criminal and civil recoveries..."⁴

Fraud-related crimes²

- About three-quarters (991) of criminal convictions involved fraud
- Fraud convictions included:
 - Conspiracy to commit health care fraud
 - Health care fraud
 - Submitting false statements related to health care matters
 - Making a false statement in regard to health care reimbursements
 - Grand larceny
 - Violations of anti-kickback statutes

Conclusion

Medicaid fraud and abuse is a serious problem that is gaining momentum. Until recently, MFCUs lacked the permission and technology to leverage the full potential of data in order to combat fraud and abuse efficiently and effectively. Most MFCUs are still exclusively reliant on fraud and abuse referrals and leads in order to respond to potential fraud cases. This data is also often delayed, incomplete, and offers only a fraction of the full picture. Fortunately, changes in legislation and advances in technology have created an opportunity for MFCUs to greatly improve their ability to detect fraud and shift the momentum back in their favor.

The HHS OIG has now empowered MFCUs to pursue data mining and will subsidize their efforts to detect fraud and patient abuse. MFCUs are now presented with a key decision: take advantage of federal funding and use the opportunity to invest in the tools and technologies that produce the highest return, or operate under the status quo.

In order to take full advantage of this opportunity, MFCUs should keep in mind some key recommendations on any claims data mining solution that they might adopt. It should:

- Investigate claims from multiple systems in a single view
- Prioritize and optimize the use of investigative resources using advanced scoring analytics, calculated from the level of suspicion and the potential exposure
- Detect fraud and abuse across claim types more efficiently and effectively
- Identify providers who habitually submit problematic claims
- Substantially increase recoveries over traditional methods
- Decrease settlement-cycle and prosecution times
- Complete more cases with existing staffing resources
- Detect patient abuse more quickly
- Expedite joint investigations with Federal staff

Today, the most innovative and effective solutions go far beyond query building—they combine Big Data with powerful rules based and predictive algorithms to deliver answers and actionable intelligence. MFCUs interested in maximizing their ability to reduce fraud and abuse should reach out to experienced partners with proven success using Big Data analytics to identify healthcare fraud. Once a MFCU's goals and objectives are matched with an appropriate solution, cost estimates can be easily calculated and a MFCU can proceed with the program application and approval process.

For more information:

Call 800.869.0751 or visit

www.lexisnexis.com/risk/healthcare

About LexisNexis Risk Solutions

LexisNexis Risk Solutions (www.lexisnexis.com/risk/) is a leader in providing essential information that helps customers across industries and government predict, assess and manage risk. Combining cutting-edge technology, unique data and advanced analytics, Risk Solutions provides products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of Reed Elsevier, a leading global provider of professional information solutions across a number of sectors.

Our health care solutions assist payers, providers and integrators with ensuring appropriate access to health care data and programs, enhancing disease management contact ratios, improving operational processes, and proactively combating fraud, waste and abuse across the continuum.

1. Source: 2012 study by a RAND analyst. <http://praescientanalytics.com/healthcare-fraud-big-data-to-the-rescue>
2. Reference: U.S. Department of Health and Human Services – Office of Inspector General; Medicaid Fraud Control Units Fiscal Year 2013 Annual Report; Daniel R. Levinson; Inspector General; March 2014; OEI-06-13-00340
3. Source: Memo from Stuart Wright; Deputy Inspector General for Evaluation and Inspections; State Fraud Policy Transmittal No. 2013-2: Elements of and Process for Submitting a Complete Data Mining Application. Rule 42 CFR 1007.20(a). http://oig.hhs.gov/fraud/medicaid-fraud-control-units-mfcu/policy_transmittals/2013-2-data-mining-application-policy-transmittal-7-1-2013.pdf
4. 2004 Program Integrity Annual Report



This white paper is provided solely for general informational purposes and presents only summary discussions of the topics discussed. The white paper does not represent legal advice as to any factual situation; nor does it represent an undertaking to keep readers advised of all relevant developments. Readers should consult their attorneys, compliance departments and other professional advisors about any questions they may have as to the subject matter of this white paper.

LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license. Other products and services may be trademarks or registered trademarks of their respective companies. Copyright © 2014 LexisNexis. All rights reserved. NXR10994-00-1014-EN-US