Tackling Fraud, Waste, and Abuse in the Medicare and Medicaid Programs

Response to the Open Letter to the Healthcare Community
December 2013

Dan Olson, CFE
Contents

I. Introduction 1
II. Recommendations 3
Recommendation 1 Expand the Traditional Healthcare Toolkit 3
Potential Savings 4
Recommendation 2 Expand the Medicare Fraud Strike Force Model 4
Potential Savings 7
Recommendation 3 Expand Integrated Data Repository 8
Potential Savings 9
Recommendation 4 Expand the Use of Public/Private Data Pooling Models 10
Potential Savings 11
Recommendation 5 Implement More Aggressive Healthcare Fraud Prescreening and Prevention Techniques 12
Potential Savings 14
Recommendation 6 Expand “Do Not Pay List” 14
Potential Savings 15
Recommendation 7 Match Vital Records to SSA and State MMIS 16
Potential Savings 17
Recommendation 8 Require Provider Re-enrollment 17
Potential Savings 18
Recommendation 9 Publish National and State Healthcare Statistics 18
Potential Savings 18
Recommendation 10 Establish Central Repository of Fraud and Abuse Cases 19
Potential Savings 19
III. Conclusion 20
On May 2, 2012, the U.S. Senate Finance Committee issued a letter to the healthcare sector soliciting industry stakeholder insights on ways to combat fraud, waste, and abuse in the Medicare and Medicaid programs. The letter followed an April 25 hearing on the effectiveness of fraud-fighting efforts at which members of the committee questioned government officials from the Department of Health and Human Services’ Office of the Inspector General, the Centers for Medicare & Medicaid Services, and the Government Accountability Office. The letter invited recommendations from the public and private sectors for program integrity and fraud and abuse enforcement reforms that would strengthen and improve current efforts to prevent and detect unlawful conduct and waste in government healthcare programs. This White Paper is a direct response to that invitation.

I. Introduction

The past four years offer examples of unprecedented partnering efforts that have served the common good by tackling healthcare fraud and abuse issues in the federal and state Medicare and Medicaid programs. The Department of Health and Human Services (HHS) and the Department of Justice (DOJ) have been at the forefront of these efforts. Early successes from their partnership have raised the hope of additional multimillion dollar fraud takedowns resulting from increased vigilance, sophisticated new technology, and harsher punishment of offenders. The HHS/DOJ partnership resulted in the single largest healthcare fraud recovery in history during Fiscal Year (FY) 2011—more than $4 billion dollars.\(^1\) This dollar amount recovery demonstrates a 58% increase over the amount recovered in FY 2009. The HHS/DOJ partnership also recovered more than $4 billion in FY 2012.\(^2\) Other statistics are impressive as well: 43% more new healthcare fraud cases were opened in 2011 than in 2010. On the state side, program integrity assessment records show that states collected more than $2.4 billion in FY 2010.\(^3\)

Despite these initial successes, we realize that a simple continuation of current initiatives will not be sufficient to fully address Medicare and Medicaid healthcare fraud. The dollar recovery amounts for Medicare and Medicaid (using 2011 and 2010 data, respectively) represent less than 1% of their overall spending. Equally important, the 2013 HHS Agency Financial Report noted that what were considered improper Medicare payments increased from $44.3 billion in 2012 to $49.9 billion in 2013.\(^4\)

The fact remains that healthcare fraud is essentially a criminal problem. The deceptive nature of fraud expands through complex relationships and multiple layers of individuals and entities that seek to protect the criminal element. Hidden within these relationships are patterns and trends that reveal the true identity of the perpetrators and the nature of their criminal acts, financial frauds and quality of care issues. Often, the conduit of the abuse remains two or more steps removed from the perpetrator. These are difficult and troubling issues.
In May 2012, six members of the U.S. Senate Finance Committee published an open letter to members of the healthcare community. In the letter, the lawmakers invited interested stakeholders to submit White Papers offering recommendations and innovative solutions to improve program integrity efforts, strengthen payment reforms, and enhance fraud and abuse prevention efforts.

New initiatives are crucial, but it is also important to leverage momentum from existing successes. This White Paper offers recommendations for both new and enhanced policies and legislation to address and prevent healthcare fraud and abuse, focusing on the following specific areas:

- Program integrity reforms to protect beneficiaries and prevent fraud and abuse
- Payment integrity reforms to ensure accuracy, efficiency, and value

### Recommendation Summary

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Potential 1st Year Savings*/Benefit</th>
<th>Potential Subsequent Savings*/Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expand Traditional Healthcare Fraud Toolkit</td>
<td>Increased federal and state fraud recoveries</td>
<td>Increased federal and state fraud recoveries</td>
</tr>
<tr>
<td>Expand Medicare Fraud Strike Force Model</td>
<td>Increased federal and state fraud recoveries</td>
<td>Increased federal and state fraud recoveries</td>
</tr>
<tr>
<td>Expand Integrated Data Repository</td>
<td>$250 million</td>
<td>$100 million</td>
</tr>
<tr>
<td>Expand Use of Public/Private Data Pooling Models</td>
<td>$250 million</td>
<td>$200 million</td>
</tr>
<tr>
<td>Implement More Aggressive Healthcare Fraud Prescreening and Prevention Techniques</td>
<td>Increased federal and state fraud recoveries</td>
<td>Increased federal and state fraud recoveries</td>
</tr>
<tr>
<td>Expand “Do Not Pay List”</td>
<td>$200 million</td>
<td>$100 million</td>
</tr>
<tr>
<td>Match Vital Records to Social Security Administration (SSA) and State Medicaid Management Information System (MMIS)</td>
<td>$100 million</td>
<td>$50 million</td>
</tr>
<tr>
<td>Require Provider Reenrollment</td>
<td>Cost avoidance</td>
<td>Cost avoidance</td>
</tr>
<tr>
<td>Publish National and State Healthcare Statistics</td>
<td>Improved resources to fight fraud and abuse</td>
<td>Improved resources to fight fraud and abuse</td>
</tr>
<tr>
<td>Establish Central Repository of Fraud and Abuse Cases</td>
<td>Improved education</td>
<td>Improved education</td>
</tr>
</tbody>
</table>

* Potential savings amounts are derived from historical reports showing dollars that were lost in similar circumstances.
II. Recommendations

Healthcare fraud is a criminal and financial problem that remains a difficult, troubling issue that requires sophisticated solutions. This White Paper offers 10 recommendations for improving federal and state efforts to combat fraud, waste, and abuse in Medicare and Medicaid programs. These recommendations focus on expanding both the traditional healthcare fraud toolkit and existing antifraud efforts through cooperation among Medicare, Medicaid, and private commercial insurance carriers to increase data pooling by removing data silos.

All recommendations in this White Paper are predicated on the following objectives:

- Protection of Medicare and Medicaid recipients’ and private payer’s privacy in accordance with provisions of the Health Insurance Portability and Accountability Act (HIPAA)
- Providers rendering high-quality services to Medicare and Medicaid recipients
- Careful stewardship of taxpayer monies that fund Medicare and Medicaid programs

**Recommendation 1  Expand the Traditional Healthcare Toolkit**

**Apply a Suite of Analytic Tools**

Due to the dynamic nature of healthcare fraud, the healthcare fraud toolkit requires a multidimensional approach that applies both prospective and retrospective analytics. Even the most sophisticated tools, if left static, will become obsolete as fraudsters work around them. Like fraud itself, our toolkit must incorporate tools that are dynamic in nature, nimble to change, and responsive to emerging patterns.

This White Paper recommends that the following suite of prospective and retrospective analytic tools be included in all payer systems to mitigate the potential of claim exploitation by the healthcare fraud perpetrator:

- Traditional business rules: logic embedded in the payer’s operating system that identifies violations of established medical guidelines or federal and state policy
- Ad hoc queries: query tool that allows a data analyst to troll the data set, perform “what if” analysis, and look for outliers that may be candidates for global anomaly routine development
- Predictive analytics: applying multiple statistical models to predict future trends and patterns in provider/recipient fraudulent behavior and to disrupt that behavior
Predictive models: conducting supervised learning, e.g., decision trees and regression analysis, and unsupervised learning, e.g., cluster analysis, with past claim or billing behavior to forecast future actions.

Link analysis: identifying relationships between providers, recipients, and billing entities through data analysis to uncover potential collusion and kickback schemes.

Clinical models: building models based on clinically supported outcomes measurement to evaluate provider treatment patterns and member outcomes in order to identify provider quality of care issues and predictors of member behavior that could result in adverse outcomes.

Inclusion of these analysis tools will provide a sophisticated and thorough analysis of claims data to thwart the would-be fraud perpetrator. However, it must be realized that the toolkit cannot stand alone; rather, it must be updated regularly and managed by a broad-based partnership that includes data analysts, investigators, auditors, medical professionals, statisticians, programmers, certified coders, law enforcement, policy experts, and attorneys.

Potential Savings

Recommendation 1 offers the potential for increasing yearly healthcare fraud recoveries well beyond the amount currently being recovered (less than 1%).

Recommendation 2: Expand the Medicare Fraud Strike Force Model

Create a Medicaid Fraud Strike Force at the State Level

Efforts to combat healthcare fraud and abuse have moved beyond the evaluation of low-hanging fruit. Increasingly sophisticated criminals use multilayered conspiracies to evade detection by healthcare fraud data analysts. New fraud techniques include money laundering using shell companies, organized crime, drug diversion, tax evasion, and kickback schemes. One example of these modern methods occurred on March 29, 2012, when a doctor and his mother were indicted for perpetrating a $1.2 million scheme involving drug distribution and tax crimes.5

The Medicare Fraud Strike Force has experienced groundbreaking success. Key to this success are the unprecedented partnering efforts among HHS, the Office of the Inspector General (OIG), the Federal Bureau of Investigation (FBI), and the Internal Revenue Service (IRS) and the employment of enhanced data analytics technology. The following examples illustrate the power of their partnering efforts in terms of monetary recoupments to federal programs:

- On September 7, 2011, 91 individuals were charged with submitting false claims ($295 million).6
- On February 17, 2012, 111 individuals were charged with submitting false claims ($225 million).7
On February 28, 2012, one physician and his accomplices were charged with submitting false claims ($375 million).8

On May 16, 2012, 107 individuals were charged with submitting false claims ($452M).9

The Medicare Fraud Strike Force recorded the single largest healthcare fraud recovery in history during FY 2011—more than $4 billion dollars.10 This accomplishment demonstrates that a dedicated partnership succeed in fighting healthcare fraud and abuse. The Medicare Fraud Strike Force is currently operating in nine metropolitan cities nationwide.11

This White Paper recommends that the Medicare Fraud Strike Force continue to be expanded at the federal level and that the following steps be implemented, allowing it to achieve continued and expanded success:

- **Continue to expand the discretionary Health Care Fraud and Abuse Control (HCFAC) program investments that are allocated to the Medicare Fraud Strike Force.** The FY 2013 discretionary budget that funds the Medicare Fraud Strike Force is $610 million. A conservative Return on Investment (ROI) is $2.00 for every $1 spent. Additional dollars allocated to the Medicare Fraud Strike Force will increase the identification of frauds committed against the Medicare program and increase the overall ROI.

- **Expand the Medicare Fraud Strike Force into additional major metropolitan areas.** Additional dollars allocated to the Medicare Fraud Strike Force will promote its expansion into additional major metropolitan areas. Such expansion efforts will continue to establish a wider net to capture and prosecute criminals, increase monetary recoupments, and improve ROI. These efforts will also lead to an increase in the sentinel effect and promote cost avoidance on the front end rather than “pay and chase” on the back end.

- **Expand the composition of the Medicare Fraud Strike Force beyond HHS, the DOJ, the OIG, and the FBI.** The addition of the Drug Enforcement Agency (DEA) and its Organized Crime Drug Enforcement Task Force, the IRS, and state licensure agencies will provide the Medicare Fraud Strike Force with partners that can identify criminal networks involved in kickback schemes, money laundering, illicit drug activity, and tax evasion.

- **Coordinate the work of the Medicare Fraud Strike Force with other Centers for Medicare & Medicaid Services (CMS) contractors.** The criminal mind is constantly looking for new ways and methods to take advantage of the payer’s system. To combat this criminal effort, the Medicare Fraud Strike Force should be enhanced by leveraging the ongoing healthcare fraud work conducted by CMS contractors, including Zone Program Integrity Contractors, Recovery Audit Contractors, Medicare Drug Integrity Contractors, and private commercial insurance carriers. Linking the data stores and data analysis techniques employed by these contractors with the investigatory and prosecution actions taken by the Medicare Fraud Strike Force will expedite the identification of emerging trends, abusive payment patterns, aberrant claims, and fraud hotspots before the perpetrators can exploit the system.
Incorporating private sector best practices. The adoption of private sector best practices that have achieved success in mitigating healthcare fraud will provide new analytics to address emerging trends. Leveraging the strengths and insights of these analytic processes will enhance the healthcare analyst’s tool set to thwart financial and quality of care issues.

This White Paper recommends that Medicaid Fraud Strike Forces be created at the state Medicaid level, thus improving the identification and collection of dollars lost to healthcare fraud, waste, and abuse. Implementation of the following steps will facilitate the implementation of Medicaid Fraud Strike Forces at the state level:

- **Establish a collective membership for each Medicaid Fraud Strike Force that includes the following entities:** state Medicaid agency, Medicaid Fraud Control Unit, Attorney General, District Attorney, FBI, DEA, IRS, professional licensing boards, Vital Records, and contractual Subject Matter Experts (SMEs). The membership includes state-level entities that mirror those on the Medicare Fraud Strike Force. Membership is strengthened through the inclusion of regulatory agencies that will assist in the identification of criminal networks involved in kickback schemes, money laundering, illicit drug activity, and tax evasion.

- **Execute data sharing agreements among all task force entities.** Data analysis is central to the identification of emerging patterns and trends that indicate potential fraud and abuse. The removal of data barriers is a prerequisite to ensuring full, free, unrestricted access to data and therefore promoting detailed claim analysis. The absence of this critical component opens doors for the criminal element and promotes their continued abuse of the Medicaid payer’s system.

- **Produce an annual report of the activity completed by the Medicaid Fraud Strike Force.** Precedent has been established for this type of report through CMS’ Medicaid Integrity Program Comprehensive Program Integrity Reviews annual report. This report highlights program weaknesses as well as noteworthy and effective practices that can be emulated by the Medicare Fraud Strike Force and state Medicaid Fraud Strike Forces.

- **Obtain enhanced Federal Financial Participation (FFP) matches to support any pilot project undertaken by the Medicaid Fraud Strike Force.** CMS provides states with a 90 percent FFP match for the design, development, installation, and enhancement of new Medicaid eligibility systems and 75% for the maintenance and operation of the system. Enhanced FFP will enable each Medicaid Fraud Strike Force to dedicate the resources required to effectively ferret out fraud and abuse in its Medicaid programs.

The removal of data barriers is a prerequisite to ensuring full, free, unrestricted access to data and therefore promoting detailed claim analysis.
Establish the respective regional CMS office as the governing entity for each Medicaid Fraud Strike Force. The 10 regional CMS offices with oversight by the Consortium for Medicaid and Children’s Health Operations (CMCHO) will provide an existing reporting structure for each Medicaid Fraud Strike Force. The CMCHO will provide uniform issue management, consistent communication, and leadership focused on achieving CMS’ strategic action plans. The Consortium Administrator for CMCHO will serve as the agent responsible for consistent implementation of the Medicaid Fraud Strike Force and policy and guidance across all 10 regions to advance the mission of each force. Establishment of this process will provide for integration to occur with the Unified Program Integrity Contractor and connect the Medicaid Integrity Program and the Medicaid Fraud Strike Force.

Create a repository to store all task force annual reports, established and maintained by CMS. A singular point of entry to access the annual reports of each Medicaid Fraud Strike Force will facilitate the sharing of states’ best practices.

The following entities will benefit through the implementation of Medicaid Fraud Strike Forces:

- CMS will benefit through an expedited implementation and adoption of Medicaid Fraud Strike Forces due to the existing structure of the Medicare Fraud Strike Force and oversight provided by the CMCHO and the 10 regional CMS offices.
- CMS has the potential to recover more improper payments associated with the federal share of Medicaid improper payments that are identified by the Audit Medicaid Integrity Contractors. The potential exists for an ROI of $7 for every $1 spent.
- State Medicaid agencies will benefit through data sharing and the identification of emerging patterns and trends.
- Medicare will benefit through regionalized issues raised and vetted at the state level and presented as actionable items at the federal level.

The synergy that would be created by a combined federal and state fraud task force could yield unparalleled success in fighting fraud and abuse.

Potential Savings

Recommendation 2 offers the potential for increasing yearly healthcare fraud recoveries well beyond the amount currently being recovered (less than 1%).
Recommendation 3 ▶ Expand Integrated Data Repository

Continue to Fund and Expand the Integrated Data Repository

The importance of the continued development and implementation of the Integrated Data Repository (IDR) cannot be overstated. The IDR and the One Program Integrity web portal—with its suite of analytic tools—have the potential to reinvent the manner in which healthcare data analytics are employed. Breaking down existing data silos and moving data into a seamless integrated system will advance the cause of healthcare fraud prevention and elevate the analysis of Medicare and Medicaid claims data to a new level.

In July 2011, the Government Accountability Office (GAO) issued Fraud Detection Systems: Additional Actions Needed to Support Program Integrity Efforts at Centers for Medicare and Medicaid Services, a report demonstrating that the IDR has been only partially rolled out and that Medicaid data has not been incorporated into the system.13 Complete system implementation is pending additional software development at the federal level and funding for states to provide their data to CMS.

CMS recently established the Medicaid and Children’s Health Insurance Program (CHIP) Business Information Solution (MACBIS) Council to develop a strategy to improve the quality and consistency of the data reported to the federal government from each state. The goal of MACBIS is to “transform Medicaid and CHIP information and data gathering, submission, storage and extraction processes from a disparate, multi-layered, non-relational and manual paper based process to an electronic, automated process.”14

This White Paper recommends that the following steps be taken to facilitate the implementation of the IDR so Medicare and each Medicaid state agency can employ it to perform data analytics:

- **Develop regionalized IDRs consistent with the 10 CMS regions.** Aligning the IDRs consistently with current CMS regions will take advantage of the existing infrastructure and minimize the disruption that a new initiative creates. The lessons learned from each regional IDR will promote a smoother and more rapid transition to the federal IDR.

- **Maintain the data protocols developed for the federal IDR and mirror them in each regional IDR.** Consistency in data protocols will minimize disruption when successful applications at the regional level are migrated for testing and implementation into the federal IDR.
Restrict the initial regionalized federal and state data loads by adopting the following approach:

- Roll out the claim-level data one date of service year at a time until testing is complete. Multiple state Medicaid data sources require the normalization of the data so it can satisfy a singular source for information-reporting requirements. Processing the data loads on a yearly basis within each regionalized area will more rapidly identify issues and promote a quicker resolution so further testing and data loads can occur.
- Roll out the claim-level data by provider type to ensure that the system is functioning properly. For example, the initial data load for each region should only include physician data. The IDR system architecture, underlying data transformations, and system logic are very complex. Evaluating the system by provider type will allow appropriate testing to identify issues and resolve them before introducing an additional provider type.
- Roll out the claim-level data within a Minimum Data Set (MDS). For example, the MDS would include up to 20 claim-level data elements that can be used to evaluate the accuracy of the data transfer to each regional IDR and the output that is generated from the IDR.
- Continually expand the data elements in the MDS after satisfactory testing has been completed for the previous MDS. This iterative process will allow appropriate testing to identify issues and resolve them before introducing additional data elements.

Conduct testing and training of each regionalized IDR with a cross-section of federal, state, and contractual SMEs. Testing by a cross-section of SMEs from multiple disciplines and backgrounds will strengthen the testing process and speed the adoption of the IDR so both Medicare and each Medicaid state agency can use it.

The benefits achieved through a regionalized approach to development include a more rapid development and a shortened testing and training cycle. The regionalized approach will promote a smoother transition to the federal IDR and therefore maximize the benefits obtained at the Medicare and Medicaid levels.

Potential Savings

Recommendation 3 offers the potential for generating $250 million or more during initial implementation and more than $100 million in subsequent years. The savings estimate is based on first-year savings generated from other Affordable Care Act (ACA) initiatives. When these changes are implemented, the savings should increase beyond these projections.
Recommendation 4  
**Expand the Use of Public/Private Data Pooling Models**

**Pool Multipayer Data Sets**
The sophisticated healthcare fraud criminal avoids the healthcare fraud radar by exploiting payers that exist in a data silo. The remedy to cure this issue is to continue to pool multiple payer data sets to provide the data analyst with a comprehensive view of the provider community. A complete view of the pooled data set provides the opportunity for analytics to identify patterns of behavior that would have been seen as isolated events if viewed through siloed data. Analytic efficiency occurs when multiple data sets are pooled to identify suspicious and abnormal data patterns. Pooled data provides a significant advantage to the healthcare data analyst in the development of comprehensive detection and prevention plans that minimize exposure to unnecessary spending.

**Healthcare Fraud Prevention Partnership (HFPP)**
The ongoing HFPP initiative combines the resources and expertise of federal and state officials, private commercial insurance carriers, and other healthcare antifraud groups. The goal of the partnership is to “perform sophisticated analytics on industry-wide data that will detect and predict fraud schemes that were previously undetectable in a fragmented healthcare system.”

HFPP anticipates that the following successes will occur:

- Expanded data set will be available for data analysis among all payers.
- Antifraud information will be shared among all payers.
- Investigators, prosecutors, policymakers, and other stakeholders will have a more complete view of an aberrant provider’s activity across multiple payers.
- Historical trends and patterns exhibited across industrywide healthcare data for all providers will enhance predictive models and their ability to identify emerging trends and promote fraud prevention.

Recently, HFPP conducted its first data exchange, and the results of the exchange were encouraging. Eleven HFPP members pooled their 44 data sources, achieving the following results:

- 1,400 misused codes were identified.
- 100 fraud schemes were identified.
HFPP promises to continue to refine and reshape the methods employed to address emerging healthcare fraud and abuse schemes across multiple payers.

**Expand Public/Private Data Pooling Programs**

This White Paper recommends that public/private data pooling programs be expanded to demonstrate the results that can be achieved through multipayer data sets. Initial success in closing loopholes in the payment system, sabotaging emerging fraudulent or abusive schemes, or terminating providers will validate the work that is being accomplished through the public/private data pooling program.

We recommend that the data pooling program implement a multitier analytical approach that continues to evolve to address the dynamic nature of healthcare fraud. Success will be achieved by concentrating efforts in geographic regions that contain a significant share of public and private covered lives in multiple plan types.

The criminal mind is constantly looking for new ways and methods to take advantage of the payer’s system. It is incumbent on the fraud control professional to incorporate public/private data pooling to expand beyond traditional methods and statistical outliers and address other potentially abusive areas. Continual vigilance, unpredictability, and sabotage at multiple data levels—transaction, group, and multiparty—will counteract the criminal mind-set. However, we must not be complacent in our continual pursuit of emerging fraudulent and abusive practices. True success will occur when the level of effort is sustained and healthcare fraud and abuse is reduced.

**Example Data Pooling Models**

Following are two examples of common data pooling models that demonstrate the results that can be achieved through multipayer data sets:

- **Excessive Hours Billed in a Day Model**: This model aggregates by day for each rendering/servicing provider ID the number of hours billed for the following time-dependent claims: 90804–90844, 90875, 90876, and 99201–99499. In order to maintain a conservative approach to data analysis, the lower threshold of the time range for each procedure code is used to calculate the hours in a day.

- **Spike Payment Model**: This model calculates a series of metrics, e.g., number of claims, number of unique recipients, dollars paid, average paid per recipient, for a specific rendering/service provider ID and compares the provider ID’s metrics for a specific time period against those of a prior time period. For example, Provider A’s paid claim data for January–June 2013 would be compared with Provider A’s paid claim data for July–December 2012.

**Potential Savings**

Recommendation 4 offers the potential for generating $250 million or more during initial implementation and more than $200 million in subsequent years. The savings estimate is based on first-year savings generated from other ACA initiatives. When these changes are implemented, the savings should increase beyond these projections.
Recommendation 5 Implement More Aggressive Healthcare Fraud Prescreening and Prevention Techniques

Adopt a Prevention-First Approach

On January 28, 2010, the first National Summit on Health Care Fraud was held in Bethesda, MD. At the summit, Acting Deputy Attorney General Gary Grindler made this telling statement during his opening remarks:

"It is not enough just to prosecute and punish health care fraud after it occurs. We must target it before it happens through aggressive pre-screening, auditing, and prevention techniques. We need to use the most effective technologies available to provide real-time access to claims data and to conduct effective data analysis so that we can detect new fraud schemes as they emerge. And we need to leverage our civil, criminal and administrative enforcement authorities along with building effective public-private partnerships."15

The significance of this statement strikes at the core of our responsibility as program integrity professionals. We must leverage the power of data analytics and statistical profiling and collaborate with public and private stakeholders and law enforcement to remain vigilant in our mission to combat and disrupt healthcare fraud and abuse.

Remain Diligent in Introducing New Techniques to Thwart the Healthcare Fraud Perpetrator

International fraud expert Dr. Malcolm Sparrow points out that the compelling nature of fraud control demands vigilance, unpredictability, and sabotage in responding to emerging patterns of fraud:18

- Vigilance: Fraud control professionals must be vigilant, always seeking new possibilities or angles that allow fraud and abuse to be identified as it is occurring and before the claim is paid.

- Unpredictability: Fraud control professionals must alter and vary their analysis techniques to keep their detection methods unpredictable, thus creating an imbalance for fraud perpetrators that will confuse and possibly defuse their planned fraudulent activities.

- Sabotage: Fraud control professionals must be nimble in order to counteract emerging fraud and abuse schemes by sabotaging them early in their development.
While each of these factors is significant individually, the combination of the three produces the best possible climate for identifying fraud and abuse and potential acts of fraud and abuse. Fraud control professionals should work diligently to achieve this optimal environment.

One prevention technique is the Provider Enrollment Predictive Modeling (PEPM) pilot. This pilot provides the Center for Medicaid and CHIP Services and state Medicaid programs with a tool that can use currently available data to predict potentially fraudulent providers prior to their enrollment in state Medicaid programs. To date, PEPM has produced strong results through sanction-based provider risk assessments that identified providers who were excluded from Medicare but not Medicaid and providers excluded in one Medicaid state but practicing in another. This model became a predictive model that can be replicated in other states.

This White Paper recommends the implementation of the following steps in order to expand existing prescreening and prevention programs:

- **Conduct background checks on all newly enrolled providers.** On March 25, 2011, CMS strengthened the provider enrollment process by expanding Sections 19–19.4, Chapter 15, of the *Medicare Program Integrity Manual*. This manual requires newly enrolled providers to be evaluated and then monitored based on one of the following three risk levels: (1) limited, (2) moderate, or (3) high. Providers classified as limited or moderate are not subject to a criminal background check. This assumption incorrectly presupposes that providers classified as limited or moderate are not likely to commit fraud. The absence of a criminal background check for providers classified as limited or moderate opens a loophole to potential fraud or abuse.

- **Enact a mandatory provider re-enrollment program to be implemented by all Medicaid agencies.** The Medicaid re-enrollment program will complement the Medicare re-enrollment program and will provide the following significant benefits:
  - Removal of nonexistent, inactive, retired, or deceased providers from the Medicaid rolls
  - Validation and update of professional licensure information for each active provider
  - Validation and update of provider demographic information
  - Validation and update of respective provider databases with current information

- **Monitor growth patterns for newly enrolled providers.** Typically, the expected growth pattern for a newly enrolled provider would be a gradual increase in claim volume, number of recipients seen per day, total dollars paid, etc. Performing anomaly detection to compare the growth pattern of a newly enrolled provider against his/her peer group’s growth pattern will identify abnormal billing patterns that might indicate a “bust-out scheme,” e.g., false claims submitted through a loophole that is being exploited.
Implement surety bond requirements for all newly enrolled providers. Medicare currently requires surety bonds for suppliers of Durable Medical Equipment, Prosthetics, Orthotics, and Supplies and Home Health agencies. Expanding the surety bond requirement to all newly enrolled providers will add a deterrent effect on would-be fraudsters. The surety bond will:

- Limit Medicare program risk to fraudulent suppliers
- Enhance the legitimacy of both the Medicare enrollment process and current suppliers
- Ensure that the Medicare program is indemnified for erroneous payments resulting from fraudulent or abusive supplier billing practices
- Ensure that Medicare beneficiaries receive reasonable products and services from legitimate suppliers

Develop predictive models that are based on quality of care issues.

Accountable Care Organizations provide coordinated care to Medicare recipients with the goal of avoiding unnecessary duplication of services and preventing medical errors. Coordination of care improves the recipient’s outcome and achieves savings for the Medicare program. Additional savings can be generated through the development of predictive models that calculate risk scores based on quality of care indexes that predict future hospitalizations or hospital readmissions. These indexes would be derived from medical conditions presented during office visits, consultations, or previous institutional care. Another example is the evaluation of systemic overbilling within Skilled Nursing Facilities. Through analysis of the entire stay of the patient—rather than a claim-by-claim analysis—cases can be discovered in which care was rendered to maximize billings rather than patient outcomes. This model should yield substantial savings through the identification of fraudulent billings.

Potential Savings

Recommendation 5 offers the potential for increasing yearly healthcare fraud recoveries well beyond the amount currently being recovered (less than 1%).

Recommendation 6 Expand “Do Not Pay List”

Expand “Do Not Pay List” to Include Retired or Sanctioned DEA Numbers

On June 18, 2010, a presidential memorandum, Enhancing Payment Accuracy through a “Do Not Pay List,” ordered the creation of a centralized database that federal agencies will be required to search before distributing payments to contractors and providers. The “Do Not Pay List” was prompted by a three-year report from federal auditors that revealed that federal agencies paid $180 million in benefits to 20,000 deceased individuals and more than $230 million to approximately 14,000 fugitives or incarcerated felons who are ineligible for benefits.
The DOJ’s Office of Drug Diversion maintains a file of all practitioners who have been assigned a DEA number. The file is updated monthly with new DEA registrants, reinstated DEA numbers, and retired DEA numbers. Fields include:

- DEA Number
- Provider Name, ID, and Address
- Date of Original Registration
- Expiration Date
- Drug Schedules
- State License Number
- State Controlled Substance Number

The following data integrity benefits will be achieved by performing a cross-match of the data in the Medicare/Medicaid claim and DEA registry:

- Validate the DEA number submitted on the claim by cross-matching it to the DEA registry.
- Confirm that the DEA number is active on the DEA registry prior to paying the claim.
- Confirm that the DEA registrant has permission to dispense prescriptions in the state of origin on the claim.
- Provide the identity of the prescriber for the instances in which the prescriber is not enrolled by Medicare or Medicaid.
- Identify claims submitted with inappropriate controlled substance authority.
- Identify claims submitted with an expired or retired DEA number.

**Potential Savings**

Recommendation 6 offers the potential for generating $200 million or more during initial implementation and up to $100 million in subsequent years. The savings estimate is based on the $180 million identified in the federal audit report. When these changes are implemented, the savings should increase beyond these projections.
Recommendation 7 › Match Vital Records to SSA and State MMIS

Enact Legislation That Requires a Nightly Data Feed from Each State Public Health Vital Records Office to the SSA Death Match File (DMF) and the State MMIS

On July 9, 2008, the U.S. Senate Subcommittee on Investigations released a report showing that between $60 million and $92 million was paid to Medicare recipients by deceased Medicare providers.23 On September 30, 2009, the GAO released a report showing that more than $700,000 was paid for controlled substances on behalf of deceased Medicaid recipients or prescribed by deceased Medicaid providers.24 Both reports reveal weaknesses in the system currently used to maintain provider and recipient date of death information.

Each state public health Vital Records office maintains death certificates that validate an individual’s date of death. Providing a nightly data feed of accurate date of death information to the SSA DMF and the state MMIS will significantly reduce the number of payments made on behalf of deceased individuals. Accurate and up-to-date recipient date of death data will allow Medicare and Medicaid claims to be rejected at the point of submission rather than after the claim is paid (the standard “pay and chase” model).

Implementation of the following steps will improve the accuracy of federal and state date of death information:

- **Establish a nightly data feed of accurate provider and recipient date of death information to the SSA DMF and the state MMIS.** The death match information will establish the basis for an edit to reject any claims presented for payment after the recipient or provider’s date of death.

- **Establish an edit that matches the claim date of service against the provider or recipient date of death to determine the validity of the claim.** Reject the claim if the date of service exceeds the date of death. Perform an analysis to recoup improper payments after the date of death.

- **Require a death indicator to be placed on the recipient’s file or the provider’s identification number when death notice is given and pend all claims until a date of death can be validated.** Perform an analysis to recoup improper payments paid prior to the death indicator being placed on the file. Reject future claims received after the valid date of death has been established.

- **Periodically cleanse the active recipient database by performing a cross-match of all eligible recipients against the SSA DMF and MMIS.** Perform an analysis to identify all claims paid after the recipient’s date of death and establish a recoupment process to recover improper payments.
Periodically cleanse the active provider file by performing a cross-match of all active providers against the SSA DMF and MMIS. Perform an analysis to identify all claims paid after the provider’s date of death and establish a recoupment process to recover improper payments. This type of fraud scheme is typically indicative of a larger scheme where the perpetrator has obtained an older provider ID and begun submitting false claims.

Accurate and up-to-date recipient and provider date of death data will allow Medicare and Medicaid claims to be rejected at point of submission rather than after the claim is paid (the standard “pay and chase” model).

**Potential Savings**
Recommendation 7 offers the potential for generating up to $100 million during initial implementation and up to $50 million in subsequent years. The savings estimate is based on the $60–$92 million identified in the Senate Subcommittee on Investigations report. When these changes are implemented, the savings should increase beyond these projections.

**Recommendation 8**

**Establish a Mandatory Re-Enrollment Program for All Medicaid Providers**

Title 42 of the Code of Federal Regulations, Section 424.515, requires all providers and suppliers who currently bill the Medicare program to enter into a five-year revalidation cycle when a completed enrollment application is submitted and validated. On March 25, 2011, CMS strengthened the provider enrollment process by expanding Sections 19–19.4, Chapter 15, of the *Medicare Program Integrity Manual.* This manual requires newly enrolled providers to be evaluated and then monitored based on one of the following three risk levels: (1) limited, (2) moderate, or (3) high. This newly enacted requirement holds promise for minimizing potential abuse in the Medicare program. The PEPM pilot is serving as a model to prevent unscrupulous providers from enrolling or re-enrolling in Medicare and Medicaid programs.

The provider enrollment process can be strengthened further by enacting a mandatory provider re-enrollment program for all Medicaid providers. This White Paper recommends that the re-enrollment program be staggered over a multiyear period by provider type in order to reduce administrative burden on individual states.

A few of the significant benefits that would be obtained from this continuous program include:

- Removal of nonexistent, inactive, retired, or deceased providers from the Medicaid rolls
- Validation and update of professional licensure information for each active provider
- Validation and update of provider demographic information
- Validation and update of respective provider databases with current information
Potential Savings
Recommendation 8 would achieve cost avoidance savings through the cleansing of Medicaid provider data through the re-enrollment process.

Recommendation 9  Publish National and State Healthcare Statistics

Calculate and Publish National and Statewide Healthcare Statistics
The DOJ, FBI, and OIG are using advanced data analysis techniques to evaluate healthcare claims. These techniques include identifying high-billing levels in healthcare fraud “hot spots” so analysts can target emerging fraud schemes. On February 28, 2012, a Texas physician and several accomplices were arrested in a nearly $375-million healthcare fraud scheme that was identified due to a fraud hot spot—fraud analysts discovered that while 99 percent of the physicians who certified patients for home health in 2010 signed off on 104 or fewer people, the indicted physician certified more than 5,000 individuals.26

This White Paper recommends that Medicare and Medicaid establish and publish fraud hot spots to provide healthcare fraud data analysts with insights into state and national standards. The development of these data models will assist in determining if potential abuses are occurring. This White Paper further recommends that the following steps be taken to provide healthcare fraud data analysts with additional information to uncover emerging schemes:

- Establish baseline thresholds by provider type at the Medicare and Medicaid level.
  Provider type thresholds will serve as peer groups for anomaly detection models. The thresholds within provider types should be based on national standard groupings, e.g., Current Procedural Terminology manual, International Statistical Classifications of Diseases Manual Version 9, or National Drug Codes.

- Update the threshold list quarterly. Regular updates to the thresholds will ensure that the claims data capture new or emerging trends exhibited in the data set. Regular updates will also enable the healthcare data analyst to evaluate current data trends against provider patterns that have been established and determined to be reasonable.

- Publish the threshold list on the CMS web site. Publication will provide ready data access to Medicare and Medicaid healthcare data analysts so they can evaluate their data against state and national standards to determine if abuse is occurring.

Potential Savings
Recommendation 9 offers the potential for increasing critical resources essential to healthcare data analysis, identifying emerging healthcare schemes, and generating additional savings for the Medicare and Medicaid programs.
**Recommendation 10 › Establish Central Repository of Fraud and Abuse Cases**

*Establish an Electronic Central Repository That Contains the Results of All Healthcare Fraud and Abuse Cases*

Multiple reports and press releases published each year provide valuable information about successful healthcare fraud investigations. Examples include the OIG Semi-Annual Report to Congress; the Health Care Fraud and Abuse Control Report; Medicare Fraud Alerts; and OIG, DOJ, and FBI press releases. Information about fraud investigations at the state level is often included in these organizations’ annual reports. Typically, the reports include details about the fraud scheme, including the type of fraud and how it was perpetrated.

This White Paper recommends the creation of a central electronic repository of all federal and state healthcare fraud cases. A few of the benefits of creating this repository include:

- Providing an educational resource for healthcare fraud analysts as they seek to learn about cases that may emerge in their regional area
- Expanding the analysts’ data mining capabilities through the inclusion of specific codes and patterns that were identified in the case
- Coordinating investigative efforts for Medicaid Health Care Fraud Prevention and Enforcement Action Team (HEAT) task forces as they implement new methods and analytics to address healthcare fraud, waste, and abuse

This White Paper recommends that the following fields be included in the data to promote searching on topics relevant to the researcher:

- Type of fraud scheme (for example, claim, multiparty, kickback)
- Type of case (Medicare, Medicaid, commercial payer)
- State of occurrence
- Provider type
- Case date

**Potential Savings ››**

Recommendation 10 will allow the healthcare fraud analyst to adopt a prevention-first mind-set through the creation of new controls identified in the electronic repository.
III. Conclusion

U.S. DOJ Assistant Attorney General Tony West recently stated:

> Ultimately, however, the role that science plays in forming our policies and practices—that will depend on each of you: your commitment; your vigilance; your dedication to ensuring that our work to create a criminal justice system that is more effective, more efficient, more just, will rest not merely on a foundation of hope, or goodwill, or good intentions, but on a bedrock of integrity born of science and research.²⁷

Partnership, in its most positive context, is a term that evokes promise, strength, and hope. Successful partnerships—collaborations of entities that share common goals—can generate a synergy that enables multiple and sometimes disparate communities to not only achieve a common good but also elevate the good to a new plateau.

The science of healthcare fraud control is incumbent on individuals engaged in active and innovative partnerships and research. Healthcare fraud is not static. The criminal mind is constantly looking for new ways and methods to take advantage of the payer’s system. This White Paper is based on continual research into healthcare fraud issues and efforts made to strengthen the existing Medicare and Medicaid system. Leveraging the knowledge and forward-thinking insights gained by federal, state, commercial insurance carrier, and contractual partners will advance the cause to improve program integrity efforts, strengthen payment reforms, and enhance fraud and abuse enforcement efforts.
About the Author

Dan Olson, CFE, has worked for more than 18 years in healthcare fraud examination, following 5 years in auditing and compliance. He is a member of the National Healthcare Anti-fraud Association, Institute of Internal Auditors, Princeton Global Networks, and the Cambridge Who’s Who. He shapes the direction of fraud prevention initiatives by serving as a charter member on the Advisory Council for the Association for Certified Fraud Examiners as well as on the Advisory Council for Harvard Business Review.

Olson serves as the SME in the application of a suite of analytic tools to identify healthcare fraud, waste, and abuse in more than 150 public and private healthcare programs. He oversees the application of data visualization tools to summarize analytic results into actionable information for healthcare programs as director of predictive analytics at HMS. His most successful applications include the use of predictive analytic algorithms and models to generate multimillion dollar savings in government programs at the Illinois Department of Healthcare and Family Services.

Olson identifies emerging healthcare trends through his research and develops prospective and retrospective algorithms to mitigate harm to the payer community. His research also serves to educate other members of the program integrity community through Vital Signs™, a national monthly healthcare fraud e-newsletter that he writes. Olson also writes healthcare fraud, waste, and abuse White Papers. His most recent—Tackling Fraud, Waste, and Abuse in the Medicare and Medicaid Programs—was written in response to the U.S. Senate Finance Committee’s request for recommendations to combat fraud, waste, and abuse in the Medicare and Medicaid programs. Previously, he wrote Using Data Analytics to Fight Fraud and Abuse: A Call to Action, offering best practices for addressing the changing tactics of healthcare fraud perpetrators.

Olson provided expert testimony before the Energy and Commerce Subcommittee on Health hearing in November 2012, “Examining Options to Combat Health Care Waste, Fraud and Abuse.” Committee Chairman Joseph Pitts also requested that Olson submit responses to Questions for the Record that may be used as the basis for future fraud and abuse legislation.

Olson welcomes comments and the opportunity for further discussion. He can be reached at 601.850.3526 or dan.olson@hms.com.
23. http://www.hsgac.senate.gov/search/?q=deceased+doctors&search-button=Search&access=p&as_dt=any&as_eq=&as_lq=any&as_oq=&as_q=any&as_sitesearch=&client=hsgac&ntsp=0&getfields=&lr=&num=15&nummgm=3&oe=UTF8&output=xml_no_dtd&partialfields=&proxycustom=&proxymode=0&proxystylesheet=default_frontend&requiredfields=&sitesearch=&sort=date%3D%3AS%3A&start=0&ud=1