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

Response to the May 2 Open Letter to the Healthcare Community

Dan Olson, CFE

June 2012

HEALTH INFORMATION DESIGNS

Contents

On May 2, 2012, the 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 25th hearing about the effectiveness of fraud-fighting efforts at which members of the committee questioned government officials from the OIG, CMS, and GAO. The letter invited recommendations from the public and private sectors for program integrity reforms that would strengthen current efforts to prevent unlawful conduct and waste involving 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 multi-million dollar fraud takedowns resulting from increased vigilance, sophisticated new technology, and harsher punishment of felons. It is well-documented that the HHS/DOJ partnership resulted in the largest annual healthcare fraud recovery in history during FY 2011—over $4 billion dollars.[1] This dollar amount recovery demonstrates a 58% increase over the amount recovered in FY 2009. Other statistics are impressive as well: the number of new healthcare fraud cases opened in 2011 shows a 43% increase from the previous year. On the state side, program integrity assessment records show that states collected over $2.3 billion in FY 2009.[2]

Despite these initial successes, we must be circumspect in feeling that a simple continuation of current initiatives will fully address Medicare and Medicaid healthcare fraud. The dollar recovery amounts for Medicare and Medicaid (using 2011 and 2009 data respectively) represent less than 1% of their overall spending. The fact remains that healthcare fraud is first and foremost 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 perpetrator(s) and the nature of their criminal act. 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 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		
Recommendation	**Potential 1st Year Savings* / Benefit**	**Potential Yearly Subsequent Savings* / Benefit**
Expand Medicare Fraud Strike Force Model	Increased federal and state fraud recoveries	Increased federal and state fraud recoveries
Expand Integrated Data Repository	$250M	$100M
Expand "Do Not Pay List"	$200M	$100M
Publicize Drug Expiration Dates	$100M	$50M
Match Vital Records to SSA and State MMIS	$100M	$50M
Require Provider Re-enrollment	Cost avoidance	Cost avoidance
Publish National and State Healthcare Statistics	Improved resources to fight fraud and abuse	Improved resources to fight fraud and abuse
Establish Central Repository of Fraud and Abuse Cases	Improved education	Improved education

*Potential savings amounts are derived from historical reports showing dollars that were lost due to similar circumstances.

II. Recommendations

This White Paper offers eight recommendations to improve federal and state efforts in combating waste, fraud, and abuse in the Medicare and Medicaid programs. The recommendations focus on expanding existing efforts through cooperation between Medicare and Medicaid and increasing data sharing by removing data silos.

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

- Protection of Medicare and Medicaid recipients' privacy in accordance with the Health Insurance Portability and Accountability Act (HIPAA)
- Delivery of high quality services by Medicare and Medicaid providers
- Stewardship of taxpayer monies that fund the Medicare and Medicaid programs

Recommendation 1 – 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. Sophisticated criminals increasingly use multi-layered 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 such example occurred on March 29, 2012 when a doctor and his mother were indicted for a $1.2 million scheme involving drug distribution and tax crimes.[3]

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

- $295M – On September 7, 2011, 91 individuals were charged for submitting false claims.[4]
- $225M – On February 17, 2012, 111 individuals were charged for submitting false claims.[5]
- $375M – On February 28, 2012, one physician and his accomplices were charged for submitting false claims.[6]
- $452M – On May 16, 2012, 107 individuals were charged for submitting false claims.[7]

This White Paper recommends that the Medicare Fraud Strike Force continue to be expanded at the federal level and be enacted at the state Medicaid level. Recommendations for the state model include:

- Collective membership: State Medicaid Agency, Medicaid Fraud Control Unit, Attorney General, District Attorney, FBI, DEA, IRS, Professional Regulations, Vital Records, and contractual subject matter experts

- Requirement to execute Data Sharing Agreements among all task force entities
- Requirement to meet at least bi-monthly
- Requirement to produce an annual report of state task force activity
- Federal Financial Participation matches to support any pilot project undertaken by the task force
- Oversight by regional CMS office
- Repository to store all task force annual reports, established and maintained by CMS

Leveraging the power of the existing Medicare Fraud Strike Force and combining this with state-level Medicaid Fraud Strike Forces could create a synergy with the potential to bring about unparalleled success in fighting fraud and abuse.

Potential Savings

Recommendation 1 holds promise for increasing yearly healthcare fraud recoveries well beyond the amount (less than 1%) that is currently being recovered.

Recommendation 2 – Expand Integrated Data Repository

Continue to fund and expand Integrated Data Repository

The singular importance of the continued development and implementation of the Integrated Data Repository (IDR) cannot be overstated. The IDR and the One Program Integrity (One PI) Web portal—with its suite of analytic tools—have the potential to reinvent the manner in which healthcare data analytics are utilized. 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 General Account Office (GAO) issued a report entitled *Fraud Detection Systems: Additional Actions Needed to Support Program Integrity Efforts at Centers for Medicare and Medicaid Services*.[8] The report showed that the IDR has been only partially rolled out and that Medicaid data has not been incorporated into the system. Complete system implementation is pending additional software development at the federal level, and funding for states to provide their data to CMS.

In the interim, this White Paper recommends the following:

- Develop regionalized IDRs consistent with the ten CMS regions. Aligning the IDRs consistently with the existing CMS regions will take advantage of the existing infrastructure and minimize the disruption that a new initiative creates.
- Maintain the data protocols developed for the federal IDR and mirror them in each regional IDR.
- Restrict the initial data load (for example, one year) until testing is complete.
- Roll out claims by provider type to ensure the system is functioning properly. For example, the initial data load should only include physician data.
- Restrict the initial roll-out to a minimum data set.
- Conduct testing and training of each database with a cross-section of federal, state, and contractual subject matter experts.

A regionalized approach to development will allow for more rapid development and shortened testing and training cycles, thereby maximizing the benefits obtained at the Medicare and Medicaid levels.

Potential Savings

Recommendation 2 holds promise for generating $250M or more during initial implementation and more than $100M in subsequent years. The savings estimate is based on first year savings generated from other Affordable Care Act initiatives. It is expected that once these changes are implemented, savings will increase beyond these projections as a result of richer data stores available to healthcare fraud data analysts.

Recommendation 3 – Expand "Do Not Pay List"

Expand "Do Not Pay List" to include retired or sanctioned Drug Enforcement Agency (DEA) numbers

On June 18, 2010, a presidential memorandum was issued entitled *Enhancing Payment Accuracy Through a "Do Not Pay List."* The memorandum 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 over $230 million to about 14,000 fugitives or incarcerated felons who are ineligible for benefits.[9]

The Department of Justice, 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 Medicare/Medicaid claims and DEA registry:

- Validation of the DEA number submitted on the claim
- Confirmation that the DEA number is active on the DEA registry prior to paying the claim
- Confirmation that the DEA registrant has permission to dispense prescriptions in the state of origin on the claim
- Identification of the prescriber for those instances where the prescriber is not enrolled by Medicare or Medicaid

Potential Savings

Recommendation 3 holds promise for generating $200M or more during initial implementation and up to $100M in subsequent years. The savings estimate is based on the $180 million identified in the federal audit report. It is expected that once these changes are implemented, cost avoidance savings will increase beyond these projections as pharmacy claims with improper DEA information continue to be rejected at the point-of-sale.

Recommendation 4 – Publicize Drug Expiration Dates

Enact legislation that requires the FDA to publish for public access the drug product expiration dates at the national drug code (NDC) level

On November 1, 2010, the OIG released a report entitled "*Review of Terminated Drugs in the Medicare Part D Program*."[10] The report indicated that CMS accepted prescription drug event (PDE) data representing over $112 million in gross drug costs associated with 2,967 terminated drugs and recommended that "CMS issue regulations to prohibit Medicare Part D coverage of terminated drugs and, in the interim, publish a list of these drugs on its Web site." CMS rejected this recommendation, stating "[the] data source used in the report methodology is likely flawed…" and "…the only authoritative source of data on final product expiration dates at the national drug code (NDC) level is data officially submitted by manufacturers to the Food and Drug Administration (FDA)."

This White Paper recommends that legislation be enacted to require the FDA to publish drug product expiration dates at the NDC level. The result of this legislation would provide Medicare and Medicaid claims processors with the authoritative FDA data source that CMS recognizes. Claims processors would have the ability to establish a data edit that rejects prescription medication at the point of sale if the dispensing date exceeds the final product expiration date.

Potential Savings

Recommendation 4 holds promise for generating up to $100M during initial implementation and up to $50M in subsequent years. The savings estimate is based on the $112 million that was identified in the OIG report. It is expected that once these changes are implemented, cost avoidance savings will increase beyond these projections as pharmacy claims for expired drugs continue to be rejected at the point-of-sale.

Recommendation 5 – 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 and the state MMIS

On July 9, 2008, the Senate Subcommittee on Investigations released a report showing that between $60 million and $92 million was paid to Medicare recipients by deceased Medicare providers.[11] On September 30, 2009, the General Accounting Office (GAO) released a report showing that over $700,000 was paid for controlled substances on behalf of deceased Medicaid

recipients or prescribed by deceased Medicaid providers.[12] 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 Social Security Administration (SSA) Death Match File and the state Medicaid Management Information System (MMIS) will significantly reduce the amount of payments made on behalf of deceased individuals. 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 5 holds promise for generating up to $100M during initial implementation and up to $50M in subsequent years. The savings estimate is based on the $60 - $92 million that was identified in the Senate Subcommittee on Investigations report. It is expected that once these changes are implemented, cost avoidance savings will increase beyond these projections as all claims that use the name of a deceased provider or recipient continue to be rejected at the point-of-sale.

Recommendation 6 – Require Provider Re-enrollment

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 5-year revalidation cycle once 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*.[13] The *Medicare Program Integrity Manual* requires newly enrolled providers to be evaluated and then monitored based on one of the following three risk levels: limited, moderate, or high. This newly enacted requirement holds promise for minimizing potential abuse in the Medicare program.

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 multi-year period by provider type in order to reduce the administrative burden on individual states.

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

- Removal of non-existent, 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 6 would bring about cost-avoidance savings resulting from the cleansing of Medicaid provider data through the re-enrollment process.

Recommendation 7 – Publish National and State Healthcare Statistics

Calculate and publish national and state-wide 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 that analysts can target emerging fraud schemes. On February 28, 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. The fraud analysts discovered that in 2010, while 99 percent of physicians who certified patients for home health signed off on 104 or fewer people, the indicted physician certified more than 5,000 individuals.[14]

This White Paper recommends that national and state-wide healthcare statistics—as well as the statistical norms used to identify provider hot spots—be published. Healthcare fraud data analysts could use this information to identify trends and aberrations that may uncover potential abuses. 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
- Update threshold list at least quarterly
- Publish threshold list on the CMS website

Potential Savings

Recommendation 7 holds promise for increasing critical resources essential to healthcare data analysis, identifying emerging healthcare schemes, and generating additional savings for the Medicare and Medicaid programs.

Recommendation 8 – 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 are published each year that provide valuable information concerning 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. In addition, information regarding fraud investigation at the state level is often included in these organizations' respective 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. The repository would provide an educational resource for healthcare fraud analysts as they seek to learn about cases that may emerge in their regional area. The repository will also expand the analysts' data mining capabilities through the inclusion of specific codes and patterns that were identified in the case.

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

- Type of fraud scheme (for example, claim, multi-party, kickback)
- Type of case (Medicare or Medicaid)
- State of occurrence
- Provider type
- Case date

Potential Savings

The electronic repository will allow the healthcare fraud analyst to promote a prevention-first approach through the creation of new controls identified in the repository.

III. Conclusion

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."

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 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, 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 over 15 years in healthcare fraud examination following five years in auditing and compliance. Mr. Olson is certified by the Association of Certified Fraud Examiners and a member of the National Healthcare Anti-fraud Association, Institute of Internal Auditors, Princeton Global Networks, and the Cambridge Who's Who.

Mr. Olson began his groundbreaking work in the program integrity field when he was tapped by the OIG of the Illinois Department of Healthcare and Family Services to be part of a charter four-member think tank called the Fraud Science Team. The goal of the team was to prevent fraud at the front end through identification techniques such as prospective editing, trending analysis, and pattern recognition. The team collaborated with Dr. Malcolm Sparrow, an international expert in the field of fraud and abuse to prevent healthcare fraud. While Mr. Olson was part of the team, CMS recognized Illinois as a best practice state, due in part to the creation of the Fraud Science Team.

In 2007, Mr. Olson accepted the position of Director of Fraud Prevention at Health Information Designs (HID). At HID, Mr. Olson continues his research in fraud prevention, and drew from his extensive program integrity background to design HID's Web-based comprehensive surveillance utilization review system (SURS), **SUR**VEIL®. Built on proven concepts and best practices, **SUR**VEIL is the first SURS solution that includes a fully-integrated case management system, allowing organizations to track potential fraud or abuse cases from the point of discovery through the disposition of the case. Mr. Olson leads HID's multi-disciplinary Fraud Informatics Technology (FIT) team in the analysis of data and the identification of potential fraud and abuse.

Mr. Olson is committed to researching trends and developments in the areas of healthcare fraud and abuse and educating other members of the program integrity community as well as external stakeholders. In April 2010, Mr. Olson authored "Using Data Analytics to Fight Fraud and Abuse: A Call to Action," a White Paper that offers best practices for addressing the aggressive and changing tactics of perpetrators. At the request of members of the Congressional Subcommittee on Health, Mr. Olson twice presented "Spotlight on State Healthcare Fraud and Abuse" in 2011. In the months following these presentations, legislative staff members have sought Mr. Olson's professional opinion on healthcare fraud and abuse issues.

Mr. Olson writes a national monthly healthcare fraud newsletter for program integrity professionals, ***SUR****VEIL Now*. Mr. Olson has been a featured speaker at the Eastern Medicaid Pharmacy Administrators Association (EMPAA) and American Drug Utilization Review Society (ADURS) conferences, presenting "The Science of Fraud Control and the Art of Discovery."

Mr. Olson also shapes the direction of fraud prevention initiatives by serving as a charter member on the Advisory Council for the Association for Certified Fraud Examiners and on the Advisory Council for Harvard Business Review.

Mr. Olson welcomes comments and the opportunity for further discussion. He can be reached at 601-420-4613 or dan.olson@hidinc.com.

About Health Information Designs

As a leader in healthcare data analysis, Health Information Designs, LLC (HID) understands the challenges faced by Medicaid agencies and healthcare programs. For over 30 years, HID has provided drug utilization review, prior authorization, prescription drug monitoring, clinical support services, and technology solutions for clients in more than 29 states.

HID's Surveillance Utilization Review System (SURS), **SUR**VEIL, provides the solution to unravel complex and sophisticated fraud and abuse strategies in the healthcare system. **SUR**VEIL is a comprehensive exception processing system designed to identify patterns and trends that may lead to potential fraud and abuse. Conceived by a team of business and technical experts, including a nationally-recognized fraud and abuse expert, **SUR**VEIL optimizes the identification of potential fraud and abuse through the prospective identification of emerging fraudulent patterns and retrospective evaluation of paid and rejected claims data.

Offices

Corporate Office

391 Industry Drive
Auburn, AL 36832
Phone: 334.502.3262
Fax: 334.466.6947

Maryland Office

213 West Main Street, Suite 204
Salisbury, Maryland 21801-4871

Corporate Web Site

www.hidinc.com

Do you need more information about fraud control?

*HID's Fraud Informatics Technology team, led by Dan Olson, CFE, produces a monthly **SUR**VEIL newsletter. If you would like to receive this newsletter, please contact Mr. Olson directly at 601-420-4613 or dan.olson@hidinc.com.*

End Notes

1. http://www.justice.gov/iso/opa/ag/speeches/2012/ag-speech-120214.html
2. https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/FraudAbuseforProfs/Downloads/fy09spiaexecsum.pdf
3. http://www.fbi.gov/seattle/press-releases/2012/south-sound-doctor-sentenced-to-more-than-12-years-in-prison-for-health-care-fraud-tax-crimes-and-drug-distribution
4. http://www.fbi.gov/news/pressrel/press-releases/medicare-fraud-strike-force-charges-91-individuals-for-approximately-295-million-in-false-billing?utm_campaign=email-Immediate&utm_medium=email&utm_source=national-press-releases&utm_content=30298
5. http://www.hhs.gov/news/press/2011pres/02/20110217a.html
6. http://www.justice.gov/opa/pr/2012/February/12-crm-260.html
7. http://www.fbi.gov/news/news_blog/strike-force-takedown-050212
8. http://www.gao.gov/new.items/d11822t.pdf
9. http://www.whitehouse.gov/the-press-office/presidential-memorandum-enhancing-payment-accuracy-through-a-do-not-pay-list
10. http://oig.hhs.gov/oas/reports/region7/70903130.pdf
11. http://www.hsgac.senate.gov/search/?q=deceased+doctors&search-button=Search&access=p&as_dt=i&as_epq=&as_eq=&as_lq=&as_occt=any&as_oq=&as_q=&as_sitesearch=&client=hsgac&sntsp=0&filter=0&getfields=&lr=&num=15&numgm=3&oe=UTF8&output=xml_no_dtd&partialfields=&proxycustom=&proxyreload=0&proxystylesheet=default_frontend&requiredfields=&sitesearch=&sort=date%3AD%3AS%3Ad1&start=0&ud=1
12. http://www.gao.gov/new.items/d091004t.pdf
13. https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNMattersArticles/downloads/MM7350.pdf
14. http://www.hhs.gov/news/press/2012pres/02/20120228d.html

