STATEMENT OF

DAN OLSON, CFE

DIRECTOR OF FRAUD PREVENTION

HEALTH INFORMATION DESIGNS, LLC

ON

EXAMINING OPTIONS TO COMBAT HEALTH CARE WASTE, FRAUD, AND ABUSE

BEFORE THE

UNITED STATES ENERGY AND COMMERCE COMMITTEE

SUBCOMMITTEE ON HEALTH

NOVEMBER 28, 2012

HEALTH INFORMATION DESIGNS

SURVEIL®

U.S. Energy and Commerce Committee
Subcommittee on Health

Hearing on Examining Options to Combat Health Care Waste, Fraud, and Abuse

November 28, 2012

Good morning Chairman Pitts, Ranking Member Pallone, and Congressional leaders. Thank you for the invitation to testify about Examining Options to Combat Health Care Waste, Fraud, and Abuse in the Medicare and Medicaid programs. I am the Director of Fraud Prevention at Health Information Designs, a national health care analytics company. I oversee our fraud and abuse detection product offering, **SUR**VEIL®, and have worked in the program integrity field for over 17 years.

Introduction

The General Accounting Office estimates that over $70 billion dollars each year are lost to health care fraud, waste, and abuse. During FY 2011, over $4 billion dollars were recovered. This amount represents the single largest health care fraud recovery in history[i], but is still less than 1% of the overall spending for the Medicare and Medicaid programs.

Health care fraud is 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. Often, the conduit of the abuse remains two or more steps removed from the perpetrator. Fraud remains a difficult, troubling issue, which requires sophisticated solutions.

A New Tool Kit

I am here this morning to present additional options to combat health care fraud and abuse—by expanding the traditional health care fraud toolkit. Due to the dynamic nature of health care fraud, our toolkit cannot be one or even two-dimensional. 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.

The tools to be considered for inclusion in our toolkit can include the following:

- Traditional business rules – incorporating claim edits based on medical guidelines or federal and state policy.
- Predictive models – using past claim or billing behavior to forecast future actions.
- Predictive analytics – developing statistical models to identify unknown data relationships.
- Link analysis – data analysis technique to identify relationships between providers, recipients, and billing entities.
- Clinical decision support systems – using claims data to determine which patients are at risk of developing major medical conditions.

We must caution against the belief that the toolkit can stand alone. The toolkit must be managed by a broad-based partnership that includes data analysts, investigators, auditors, medical consultants, statisticians, programmers, certified coders, law enforcement, policy experts, and attorneys.

Expand Current Efforts

We have made significant progress to combat health care fraud, waste and abuse. The following areas can be expanded to generate additional savings for the Medicare and Medicaid programs.

- **Expand the Medicare Fraud Strike Force at the federal level and enact it at the State level.** The Medicare Fraud Strike Force has experienced groundbreaking success during the past year. Expansion of the Strike Force model to the state level with oversight by each regional CMS office will expand the current 1% recovery of federal and state dollars lost to health care fraud.

- **Continue to fund and expand the Integrated Data Repository.** The goal of the Integrated Data Repository (IDR) is to create a database that contains multiple years of Medicare and Medicaid data. 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*.[ii] 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. I recommend that CMS adopt a regionalized approach to development that will allow for more rapid development and shortened testing and training cycles. Expansion of the IDR could generate $250M or more during initial implementation and more than $100M in subsequent years.

- **Expand the "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. Currently, the "Do Not Pay List" does not include a cross-match of the data in the Medicare/Medicaid claim and DEA registry. I recommend that validation of the DEA numbers occur prior to payment. This recommendation could generate savings of $200M or more during initial implementation and up to $100M in subsequent years.

- **Calculate and publish national and state-wide health care statistics.** The DOJ, FBI, and OIG are using advanced data analysis techniques to evaluate health care claims. These techniques include identifying high-billing levels in health care fraud "hot spots," so that analysts can target emerging fraud schemes. I recommend that access to the national fraud hot spots be published so that health care fraud data analysts can gain insights into national standards and determine if potential abuses are occurring. I further recommend that the following steps be taken to provide health care fraud data analysts with additional information to uncover emerging schemes.
  - Establish baseline thresholds by provider type at the Medicare and Medicaid level
  - Update the threshold list at least quarterly
  - Publish the threshold list on the CMS website

This recommendation holds promise to increase critical resources essential to health care data analysis, identify emerging health care schemes, and generate additional savings for the Medicare and Medicaid programs.

I would be happy to expand on any of the above items during our question and answer time.

Conclusion

Thank you, Chairman Pitts, Ranking Member Pallone, and Congressional leaders for this opportunity to present. I have written two white papers that address this subject in more detail and have provided these as appendices to my written testimony. At this time, I will be happy to answer any questions.

---

i. http://www.justice.gov/iso/opa/ag/speeches/2012/ag-speech-120214.html
ii. http://www.gao.gov/new.items/d11822t.pdf

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

Using Data Analytics to Fight Fraud and Abuse:
A Call to Action

Dan Olson

with Connie Lewis, MBA

April 2010

HEALTH INFORMATION DESIGNS

Contents

Recent federal directives have turned a national spotlight on the issue of fraud and abuse in the health care system. In this paper, the author—a distinguished member of the Program Integrity community—explains that the only recourse for fraud control professionals is to continually alter their methods and tactics to stay one step ahead of perpetrators. Advancements in information technology, coupled with expert logic, provide improved methods for targeting and identifying fraud, and recouping damages. Using these methods, fraud control professionals should move beyond the status quo and stay poised to fight fraud not only as it exists but as it emerges.

I. Background

The year 2009 will be remembered for the historic strides that took place in the examination of the health care industry. The debate on health care reform permeated the news media on a routine basis as congressional leaders researched, debated, and worked to craft a federal plan that would serve the neediest constituencies.

The debate appropriately cast a spotlight on health care fraud and abuse, bringing the issue to national attention. On January 28, 2010, the first National Summit on Health Care Fraud was held in Bethesda, Maryland. At the summit, Acting Deputy Attorney General Gary Grindler provided 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.*[1]

Less than two months later, President Barack Obama issued a memorandum to increase the collection of improper health care payments through "Payment Recapture Audits," described as audits conducted using state-of-the-art technology and expert professionals to ferret out fraud and abuse.[2] The potential recovery from this effort is anticipated to be at least $2 billion over the next three years.

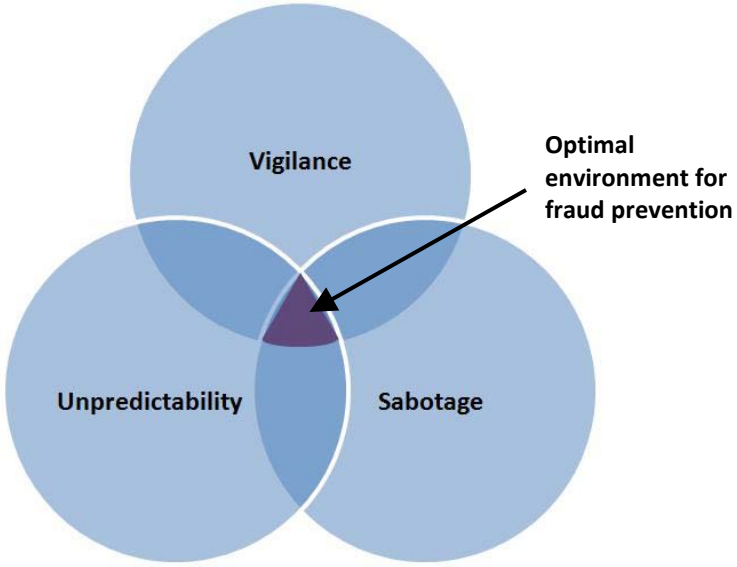
The recent directives regarding health care fraud and abuse represent a direct **call to action**. While fraud control professionals should continue their standard operating procedures, they must not be complacent with maintaining the status quo. Instead, program integrity departments must strengthen their efforts by finding new approaches and angles to identify and prosecute fraud and abuse cases, and proactively prevent future cases. The remainder of the paper is dedicated to explaining the optimal approach to fighting fraud using **data analytics**, which integrates advanced database technology with expert, industry-based logic.

II. Vigilance, Unpredictability, and Sabotage

Health care *fraud* amounts to the intentional misrepresentation of a material fact on a health care claim in order to persuade the payer to process and pay a false claim. Health care *abuse* is a disregard for accepted business or medical practices in order to obtain a greater claim reimbursement.

Traditionally, both fraud and abuse were identified through analysis of paid claims data. This approach is not enough. Today's fraud control professionals cannot simply perform static, post-payment reviews. A contemporary and comprehensive approach must utilize multiple approaches to address emerging issues of fraud and abuse to thwart would-be perpetrators from siphoning Medicare and Medicaid dollars from needy citizens. As fraud expert Dr. Malcolm Sparrow points out, the compelling nature of fraud control demands vigilance, unpredictability, and sabotage in responding to emerging patterns of fraud.[3]

- **Vigilance** – The fraud control professional must be vigilant—ever-seeking new possibilities or angles that allow fraud and abuse to be identified as it is occurring and before the claim is paid. Without vigilance, the fraud control professional becomes complacent in relying on methods of fraud control that worked in the past, without modifying or supplementing these to address new methods used by fraud perpetrators.
- **Unpredictability** – Predictable—or static—patterns of behavior on the part of the fraud control professional provide an opportunity for innovative fraud perpetrators to develop schemes that will leech untold dollars from payers. Conversely, unpredictable or creative patterns of behavior create an imbalance for fraud perpetrators that will confuse and possibly defuse their planned fraudulent activities. Fraud and abuse control professionals must alter and vary their behavior to keep their detection methods unpredictable.



- **Sabotage** – The fraud control professional must be nimble, in order to counteract emerging fraud and abuse schemes by sabotaging them early in their development. Various forms of sabotage are effective in subverting the activity of a perpetrator. For example, one method (that will quickly elicit a response from the perpetrator) is to suspend payments pending a review of claims. The fraud control professional can also work with law enforcement officials to coordinate undercover work to build a case against the perpetrator.

While each of these factors is significant individually, the combination of the three produces the best possible climate for identifying cases of fraud and abuse and potential acts of fraud and abuse. Fraud control professionals should work diligently to achieve this optimal environment. The absence of these factors will provide a greater opportunity for a fraud perpetrator to exploit the weaknesses of health care payment systems.

III. Using Data Analytics to Detect and Prevent Fraud

Fraud control in the health care system involves the objective, careful, and systematic study of health care data. By running large amounts of data against algorithms carefully crafted to uncover unscrupulous acts, analysts can pinpoint cases of potential fraud or abuse for follow up and further investigation.

The answers are in the data.

It has been aptly said that the "answers are in the data." While simply put, this is a profound truth. However, data will reveal the correct answers only when the correct questions are asked and the results are properly evaluated. The following points should guide the work of data analysis:

- What are the key questions that need to be asked?
- How should the data be evaluated?
- How much effort should we expend to find answers?

Asking the Right Questions

For each submitted claim, the fraud control professional must ask several key questions to begin the evaluation process.

Is this a valid claim? In the most elementary sense, a valid claim is one that passes successfully through claims processing front-end edits. However, to determine real validity, the fraud control professional must continue questioning.

Is the claim legitimate? In other words, was it properly submitted for medically-necessary services rendered on behalf of a beneficiary? To determine the validity of a submitted claim, the claim must be evaluated within its context, which encompasses the services surrounding the claim submittal and the claim demographic. If the surrounding services are consistent with the claim in question and comply with medical standards, then the claim's validity is increased. However, if there are inconsistencies in the surrounding services, then the fraud control professional should question the claim's validity. The claim demographic can take on many layers, such as transaction type (e.g., professional, institutional, pharmaceutical); provider type (e.g., pharmacy, laboratory); or beneficiary category of eligibility (e.g., illegal alien, working disabled). Inconsistencies in the claim demographic, when taken in context with the surrounding services, should cause the fraud control professional to question the claim's validity. The context of the claim is critical in determining the validity of the claim submittal.

Is the claim a legitimate claim in relation to the payer's payment policy? Policy manuals, provider handbooks, state and federal regulations, etc. dictate the proper method of payment for a claim. Embedded within the payment policy are business rules that define procedures,

thresholds and limits for the payment of the claim. The payment policy is the linchpin that defines the proper payment edit structure. Consistency between the payment policy and the payment edit structure is monumental when validating a claim. When consistency breaks down, loopholes are created and the payer's system becomes vulnerable for potential fraud and abuse.

Using the Right Methods

It is important to remember that each claim is unique. However, beyond this uniqueness, a body of claims will exhibit characteristics that allow the fraud control professional to explore the data and look for revealing trends and patterns of behavior. These trends and patterns become the basis for discovering predictive behavior that will lead to unraveling an emerging fraud or abuse scheme before it occurs.

Trends and patterns on their own do not necessarily indicate bad or flawed behavior. For instance, one might find that a provider's or clinic's billing practice will only submit claims for payment at the end of each month. On its own, this may not reveal a questionable practice, especially if the dates of service for these claims occurred in the previous 30 – 60 days. However, the results of the analysis would change if the dates of service were consistently for claims eight to twelve months old, or perhaps for claims that had been previously rejected multiple times.

Traditional surveillance utilization review systems' (SURS) exception processing will allow the fraud control professional to identify statistical outliers based on standard deviations. A statistical outlier in its purest form is data (or claims) that have separated themselves from the normal distribution of the data. The separation of data could occur at the upper- or lower-bound of the data spectrum. For example, an exception process might identify family practitioners who exceed the standard deviation and consistently submit claims for the most expensive established office visit procedure code, i.e., 99215.

Recently, the Medicare Fraud Strike Force used this process to identify statistical outliers that exceeded the national averages for specific claims. The Medicare Fraud Strike Force called these aberrations "fraud hot spots." For example, when the Strike Force calculated the amount paid per beneficiary for inhalation drugs in Miami and compared it to the national average, they discovered that Miami exceeded the national average by 3,000%. The Strike Force also calculated the number of eye tests performed in Houston and compared it to the national average for eye tests performed, finding that the number of eye tests performed in Houston exceeded the national average by 2000%.[4] 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 expand beyond statistical outliers to address other potentially abusive areas.

The criminal mind is constantly looking for new ways and methods to take advantage of the payer's system.

The vigilant fraud control professional must implement a multi-faceted approach to evaluate the data. The following are examples of areas in which research should be expanded:

- **Inter-relationships** – This area involves evaluating a beneficiary's relationship with multiple providers to identify a potential kickback scheme or duplicate billings. The kickback scheme may be identified through examination of the provider-beneficiary relationship. For example, analysis of a nursing home may result in a discovery that all beneficiaries are treated by the same physician clinic, serviced by the same transportation company, and receive medications from the same pharmacy. Further review may determine that ownership interests are intertwined between all providers involved or that kickbacks are being given to secure a provider's business.

  A duplicate billing scheme can also be identified through examination of the provider-beneficiary relationship. A cluster of beneficiary claims for the same service may be submitted by several providers on the same date of service. The perpetrator may try to disguise the duplicate billings by submitting claims for payment at different times, e.g., different months. A second example may be identified when a beneficiary list is passed around a clinic or group practice, and claims are submitted by multiple providers for the beneficiaries with the same procedure code on the same date of service.

- **Newly Enrolled Provider Monitoring** – This area involves evaluating newly-enrolled providers within the bounds of their provider type. Knowledge of the data is essential in order to understand the typical growth pattern that a newly-enrolled provider may exhibit within their provider type. The analysis would begin once the newly-enrolled provider begins to submit claims. Providers would be flagged for review at any point they exceeded the growth pattern during the evaluation period.

- **Quality of Care** – This area involves examining beneficiary claims to determine if the beneficiary received an established standard of care for their medical condition. For example, an expectant mother should receive a minimum number of office visits, sonograms, and lab tests during the course of her pregnancy. If these standards are not met, then a quality of care issue could be raised. Quality of care can also be reviewed in a managed care environment to determine if an underutilization of services occurred.

Continual vigilance *… will counteract the criminal mindset.*

Would-be perpetrators will initially be caught off-guard by these approaches, but they will quickly adapt and redirect their criminal activity to new areas of exploitation. It is important to note that a multi-tier analytical approach must be ongoing. Continual vigilance, unpredictability, and sabotage at multiple data levels—transaction, group and multi-party—will counteract the criminal mindset.

Expending the Right Efforts

Achieving success in the identification of health care fraud and abuse is dependent upon the level of effort and resources that are allocated. A commitment to the acquisition of proper technologies, the proper staffing, and a far-reaching think-tank approach will garner success in derailing fraudulent and abusive activity.

- **Proper Technologies** – The acquisition of effective technologies that provide real-time access to data and conduct effective data analysis is an essential step in subverting health care fraud and abuse. These tools must have the ability to use data analytics to perform statistical analysis at multiple levels to reveal aberrant behavior and facilitate predictive modeling. The ability to drill down to the claim line detail to identify the claim demographic is inherent in this process. The technology must also have the ability to efficiently track all segments of activity on each case from inception through disposition.
- **Proper Staffing** – The establishment of multiple partnerships among government, law enforcement, and fraud control professionals creates a synergy that will lead to increased integrity efforts and advance the overall cause of fraud prevention. Development of a prevention-first mindset will lead to an efficient and effective avenue to identify fraud and abuse schemes as they emerge.

Initial success in closing loopholes in the payment system, sabotaging emerging fraudulent or abusive schemes, or terminating providers will validate the work that has been accomplished. Caution must be taken to avoid complacency in the continual pursuit of emerging fraudulent and abusive practices. True success will occur when the level of effort is sustained and health care fraud and abuse is reduced.

IV. Conclusion

Agencies are under great pressure to reduce health care costs by not only recovering improper payments, but by stopping fraud and abuse before it occurs. This cannot be done without investing in the best technological tools available and employing expert fraud control professionals to harness them. A contemporary and comprehensive approach to fraud control incorporates data analytics to discover issues as they emerge, track perpetrators, and ultimately recover overpayments.

Fraud control professionals must leverage the power of data analytics and statistical profiling …to combat and disrupt emerging issues in health care fraud and abuse.

Returning to Acting Deputy Attorney General Grindler's statement:

> *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.*

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 stakeholders and law enforcement, to provide an intentional vigilance in our mission to combat and disrupt emerging issues in health care fraud and abuse.

▪▪

About the Author

Dan Olson has worked for over a decade in fraud examination following five years in auditing and compliance. Mr. Olson began his groundbreaking work in the program integrity field when he was tapped by the Office of Inspector General (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 was to prevent fraud at the front end through identification techniques such as prospective editing, trending analysis, and pattern recognition. While Mr. Olson was part of the team, the Centers for Medicare & Medicaid Services (CMS) recognized Illinois as a best practice state due in part to the creation of the Fraud Science Team.

Mr. Olson is known in the national program integrity arena for authoring a White Paper in 2005 that provided recommendations to improve the integrity of the National Provider ID. While in Illinois, he also served as a charter member of the Medicaid Fraud Prevention Executive Workgroup, performing pharmaceutical research and developing several prospective edits that saved the State of Illinois millions of dollars.

Currently the Director of Fraud Prevention at Health Information Designs, Inc. (HID), Mr. Olson is a member of the Association of Certified Fraud Examiners, the Institute of Internal Auditors and the Princeton Global Networks. Within the past year, Mr. Olson was a featured speaker at the National Association for Medicaid Program Integrity (NAMPI) annual conference and presented "The Science of Fraud Control and the Art of Discovery" at the Eastern Medicaid Pharmacy Administrators Association (EMPAA) and American Drug Utilization Review Society (ADURS) annual conferences.

Dan Olson's work with fraud prevention logic provides the ideal background for designing technology to detect, address, and prevent fraud. Since moving to HID in 2007, Mr. Olson has employed his impressive background in program integrity to design HID's comprehensive Web-based SURS and Case Management solution, **SUR**VEIL™. Built on proven concepts and best practices, **SUR**VEIL is the first solution to integrate a full case management system within a surveillance utilization review system, allowing organizations to track potential fraud or abuse cases from the point of discovery through the disposition of the case.

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, Inc. (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 20 states.

HID's **SUR**VEIL™ Surveillance Utilization Review System (SURS) 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

Mississippi Office

513 Liberty Road, Suite 2A
Flowood, Mississippi 39232

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 Team, led by Dan Olson, 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. U.S. Department of Health and Human Services and U.S. Department of Justice, "Stop Medicare Fraud," (http://www.stopmedicarefraud.gov/healthcarefraud.html)

2. Presidential Memorandum Regarding Finding and Recapturing Improper Payments, March 10, 2010. (http://www.whitehouse.gov/the-press-office/presidential-memorandum-regarding-finding-and-recapturing-improper-payments)

3. Sparrow, Malcolm K. *The Character of Harms: Operational Challenges in Control.* Cambridge University Press, 2008

4. Prepared comments by Assistant Attorney General Lanny Breuer at the 2009 National Health Care Anti-Fraud Association Conference on November 18, 2009.