

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

**Dan Olson**

with Connie Lewis, MBA

April 2010

## Contents

<b>I. Background .....</b>	<b>1</b>
<b>II. Vigilance, Unpredictability, and Sabotage .....</b>	<b>2</b>
<b>III. Using Data Analytics to Detect and Prevent Fraud.....</b>	<b>3</b>
Asking the Right Questions.....	3
Using the Right Methods.....	4
Expending the Right Efforts.....	5
<b>IV. Conclusion.....</b>	<b>6</b>

*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.<sup>1</sup>*

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.<sup>2</sup> The potential recovery from this effort is anticipated to be at least \$2 billion over the next three years.

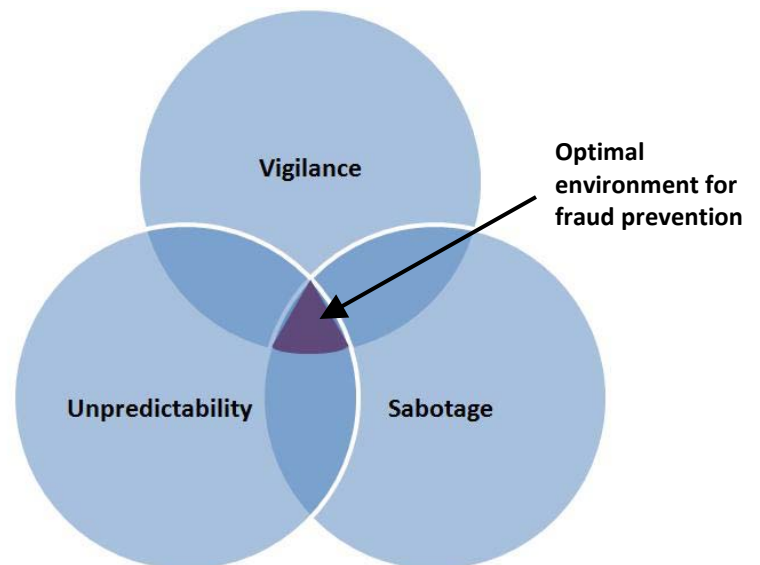
The recent directives regarding health care fraud and abuse represent a direct **call to action**. While fraud control professionals should continue their standard operating procedures, they must not be complacent with maintaining the status quo. Instead, program integrity departments must strengthen 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.<sup>3</sup>

- **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

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

average for eye tests performed, finding that the number of eye tests performed in Houston exceeded the national average by 2000%.<sup>4</sup> 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 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.

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.*

*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.*

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, **SURVEIL™**. Built on proven concepts and best practices, **SURVEIL** 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](mailto: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 **SURVEIL™** Surveillance Utilization Review System (SURS) provides the solution to unravel complex and sophisticated fraud and abuse strategies in the healthcare system. **SURVEIL** 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, **SURVEIL** 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](http://www.hidinc.com)

***Do you need more  
information about fraud  
control?***

*HID's Fraud Informatics Team,  
led by Dan Olson, produces a  
monthly **SURVEIL** newsletter.  
If you would like to receive this  
newsletter, please contact Mr.  
Olson directly at 601-420-4613  
or [dan.olson@hidinc.com](mailto: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.