Paper 1769-2014

Making It Happen: A Novel Way to Combine, Construct, Customize, and Implement Your Big Data with SAS® Data Discovery, Analytics, and Fraud Framework in Medicare

Vivek Sethunatesan, Technical Advisor – Health IT, Northrop Grumman, Baltimore, MD

ABSTRACT

A common complaint from business users working on identifying fraud and abuse in Medicare is that teams focus on operational applications, static reports, and high level outliers, but when faced with the need to constantly evaluate changing Medicare provider and beneficiary/enrollee dynamics, those business units clamor for more dynamic and accurate detection approaches. Providing these organizations with a data discovery and predictive analytics framework that leverages Hadoop and other big data analytical approaches, while providing a clear path for rapid fact-based decisions, is critical in pre- and post- payment fraud and abuse analysis. This paper describes the data management, data discovery, predictive analytics, and social network analysis capabilities that are included in the fraud framework, and how a unified approach can significantly reduce the analytical life cycle of building and deploying fraud models.

INTRODUCTION

Section 4241 of the Small Business Jobs Act of 2010 (Public Law 111-240) mandates the use of predictive modeling and other analytic technologies to identify and prevent fraud, waste, and abuse in the Medicare Fee-for-Service (FFS) program. The loss of taxpayer dollars through waste, fraud, and abuse drives up healthcare costs. The Centers for Medicare & Medicaid Services (CMS) is pursuing an aggressive program integrity strategy that will prevent fraudulent transactions from occurring, rather than simply tracking down fraudulent providers and pursuing fake claims. Reversing the traditional pay-and-chase approach to program integrity is the main goal of the National Fraud Prevention Program.

When organizations pursue a long-term sustainable approach that incorporates innovative technologies in integrated solutions, a reusable services-based data discovery and predictive analytics framework architecture approach enjoys greater success in supporting data management, reporting, and analytics demands, and in quickly turning models into prioritized alerts that avoid improper or fraudulent payments. This paper discusses an enterprise fraud framework and its components that enables organizations to define efficient and effective models to address complex schemes; identify and remediate fraud, waste, and abuse vulnerabilities; and shorten triage efforts using a variety of data sourced from big data platforms like Hadoop and other relational database management systems.

This paper assumes the reader has a basic understanding of Medicare; healthcare fraud, waste, and abuse terminology; base SAS® programming; the relational database management system; the Hadoop data file system platform; and protocols to access data from Hadoop.

MEDICARE FRAUD PREVENTION PROCESS

Medicare fraud and abuse is a serious problem. Although the majority of healthcare providers are honest and well-intentioned, a minority of providers intent on abusing the system can cost taxpayers billions of dollars and put beneficiaries' health and welfare at risk. The impact of these losses and risks is magnified by the growing number of people served by Medicare and the increased strain on Federal and state budgets. Preventing fraud in Medicare involves striking an important balance: carrying out the core responsibility to protect beneficiary access to necessary healthcare services and reducing the administrative burden on legitimate providers and suppliers, while ensuring taxpayer dollars are not lost to fraud, waste, and abuse.

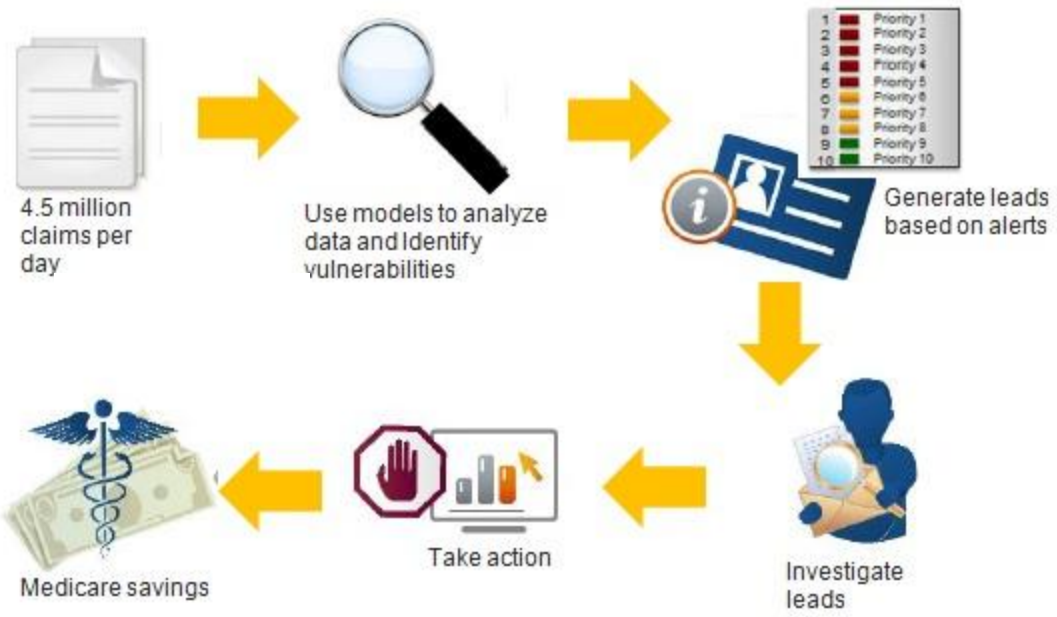

Figure 1. Medicare Fraud Prevention Process

As shown in Figure 1, the Medicare fraud prevention process analyzes information from multiple Medicare and other data sources to predict whether observed billing patterns or trends are likely to be fraudulent. The process runs predictive models against all Medicare Part A and Part B claims nationwide to detect aberrant billing patterns and other potential vulnerabilities using predictive analytics—sophisticated mathematical and statistical algorithms and models—to identify suspicious behavior. CMS may take a variety of administrative actions based on the results of investigating leads, including implementation of claims processing edits, claim denials, prepayment review, payment suspensions, revocation of Medicare billing privileges, and referral to law enforcement. These actions result in savings to the Medicare Trust Funds.

WHY USE A FRAUD AND ABUSE FRAMEWORK?

A reusable fraud and abuse framework is necessary to implement an efficient, effective, and scalable Medicare fraud prevention process. This framework provides a collaborative environment for a multi-disciplinary team to develop consistent approaches for statistical and sophisticated data analysis to identify and prevent fraud and abuse. A unified fraud and abuse framework addresses some of the common challenges listed below.

- **Siloed Business Unit**: Different departments often use disparate legacy solutions that don't talk to each other, making it almost impossible to share information and spot suspicious activity across the organization.
- **Staff Limitations**: There aren't enough analysts to investigate all suspicious activity, and scoring based on rules alone generates too many false positives, which consume valuable analyst time.
- **Poor Data Quality**: Disparate systems and the inability to integrate third-party data or text data mean that information is often incomplete and unreliable.
- **Changing Tactics**: Fraudsters actively test rules and thresholds, and constantly change elements of their identities, making it hard to match a claim with a known fraudster.
- **Limited Scope**: Current data models rarely produce a view beyond a single patient identity. The lack of an Enterprise approach to fraud, waste, and abuse makes it hard to spot high-risk relationships and get a full picture of a patient, claims, and all related entities.

FRAUD AND ABUSE FRAMEWORK COMPONENTS

A fraud and abuse framework combines many individual components that address specific use cases to support a comprehensive set of vital tasks to prevent, reduce, and address fraud and abuse. These components work in a unified approach that can significantly reduce the analytical life cycle of building and deploying fraud models using the SAS Fraud Framework set of tools. This framework is fully customizable; the audience can chose specific components of this framework to suit their specific implementation needs.

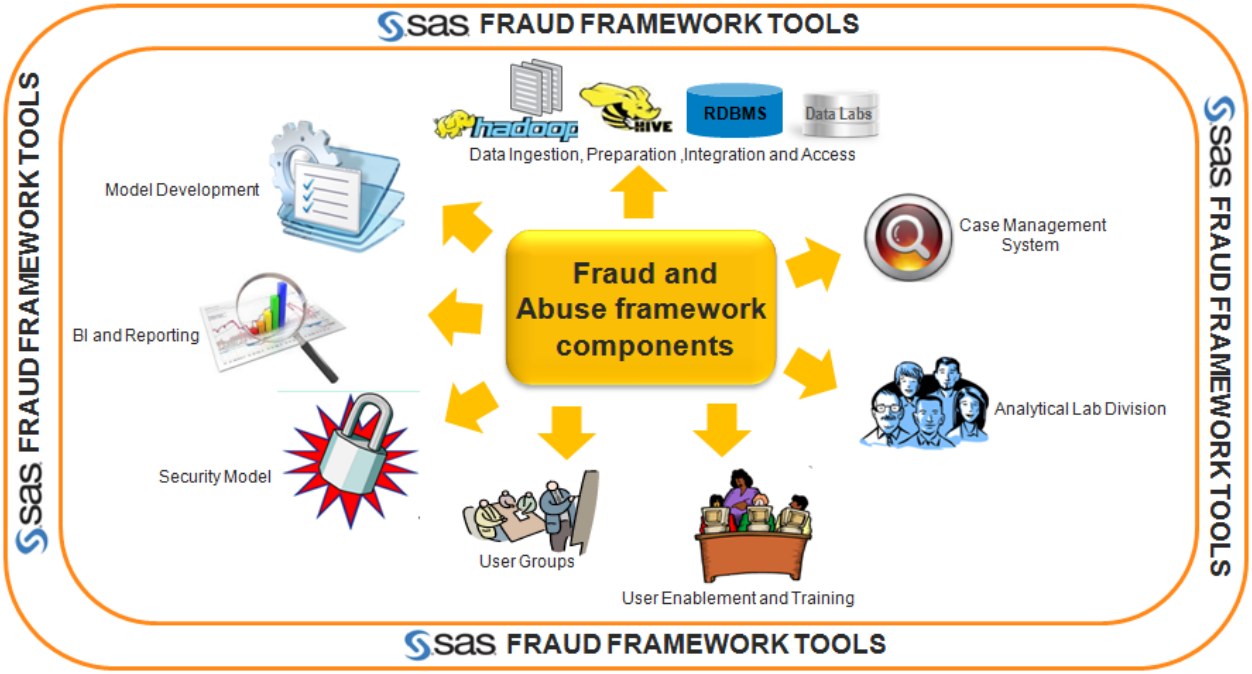

Figure 2. Fraud and Abuse Framework Components

As shown in Figure 2, the Medicare Fraud and Abuse framework is a combination of components that address specific use cases supporting data management, reporting, and analytics demands. These components quickly turn models into prioritized alerts that avoid improper or fraudulent payments. They are customizable to meet the needs of the user, and can also be used to support user training, on-boarding, user roles, and security.

SAS FRAUD FRAMEWORK TOOLS

The SAS Fraud Framework consists of software products designed to detect and prevent fraud, waste, and abuse for organizations in banking, government, healthcare, and insurance. The SAS Fraud Framework Toolset for HealthCare is an end-to-end framework for detecting, preventing, and managing healthcare claims fraud.

The SAS Fraud Framework is also a system for continuous learning and improvement. As fraud schemes evolve and morph over time, it is essential that prevention and detection system evolve and morph with them. Each time an alert is triggered or a vendor eligibility referral is passed, the results are stored within the Intelligent Fraud Repository as known outcomes. The predictive models used in the framework access this repository of known outcomes as they apply analytic approaches used in a previous similar approach. By registering and leveraging known outcomes in the repository, future fraud payments can be intelligently stopped. This feedback loop allows the SAS Fraud Framework to continue to learn and be more precise with risk scoring. Specifically, it raises more alerts on entities and networks that have attributes similar to confirmed, known bad providers and submitters. With this feedback loop in place, the Fraud Framework and associated analytical approaches continuously evolve as new fraud schemes are detected and uncovered. This knowledge becomes part of the Fraud Framework, and is automatically and instantly applied going forward.

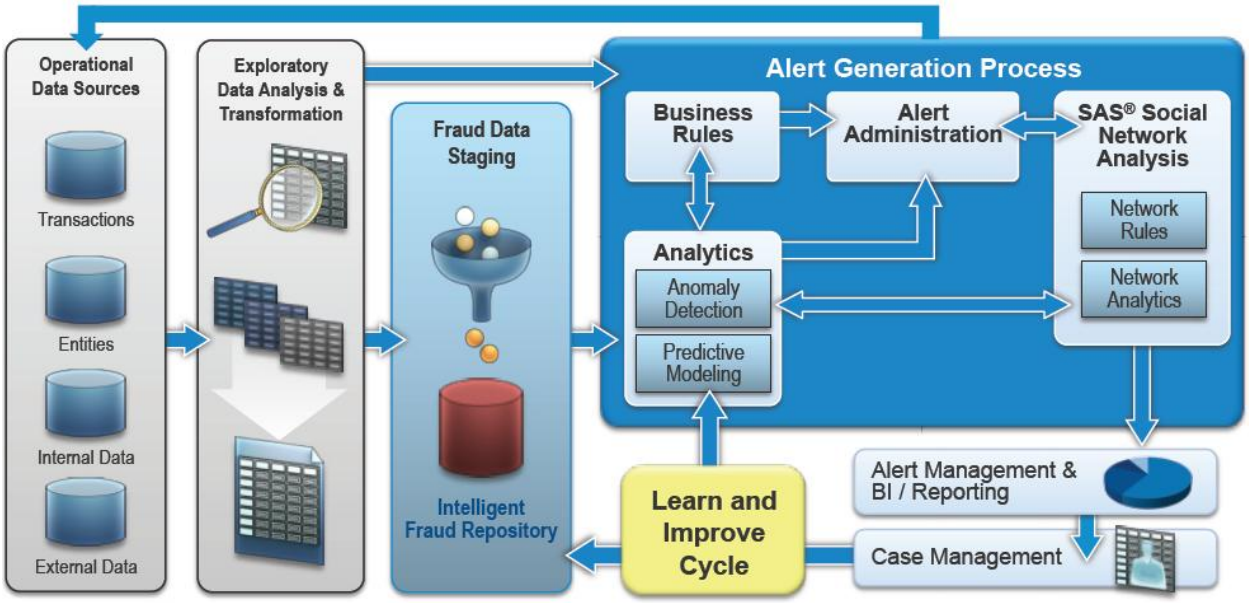

Figure 3. SAS Fraud Framework Process Flow

As shown in Figure 3, the SAS Fraud framework process flow is a combination of components that address specific use cases supporting data management, fraud detection, reporting, analytics, and case management demands to detect and prevent both opportunistic and professional fraud at each stage of the claims process.

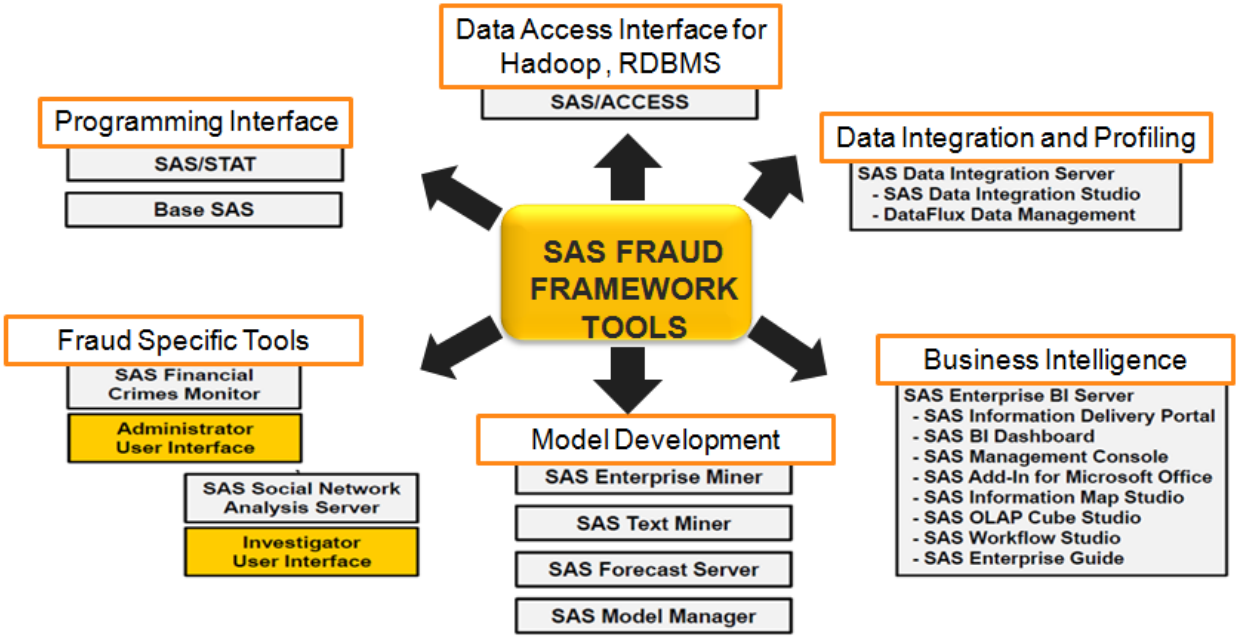

Figure 4. SAS Fraud Framework Toolset

As Figure 4 illustrates, The SAS Fraud Framework Toolset includes:

- Fraud-specific Tools: Fraud-specific components for fraud detection, lead generation, alert management, and integrated case management system user interface.
    - Calculate the propensity for fraud at first submission, then rescore claims at each processing stage as new

claims data is captured.
    - Incorporate fraud detection methods into the process at the most appropriate points – e.g., cases where anomaly detection scenarios may require data that is not available until later in the adjudication process.
    - Prioritize the investigative order of alerts by scoring alerts in real time, based on the specific characteristic.
    - Route alerts to appropriate team members based on user-set rules and requirements.
    - Go beyond transaction and account views to analyze related activities and relationships at a network dimension.
    - Produce complete dossiers of networks surrounding a case and gain fast access to full details on all related parties and networks.
- Data Integration and Data Quality/Profiling Tools:
    - Consolidate historical data from internal and external sources – claims systems, watch lists, third parties, unstructured text, etc.
    - Eliminate or reduce redundant or inconsistent data with the solution's built-in data profiling/quality tools.
    - Seamlessly integrate the solution with your third-party fraud applications.
- Business Intelligence (BI) Tools:
    - Use the SAS Enterprise Business Intelligence toolset to access and use data, and interpret it into meaningful information by generating quality reports that can be used to:
        - Monitor model performance
        - Review investigator workload
        - Monitor activities, actions, and rulings
- Data Access Interface to connect to Hadoop and other relational database management systems.
- Model Development and Monitoring Client Tools:
    - Create and logically manage business rules, analytic models, alerts, and known fraudster lists.
    - Customize analytic models to identify fraud, waste, and abuse not found by existing business rules.
    - Easily manage the deployment, aggregation, scheduling, suppression, and routing of similar rules across multiple factors, such as parties, Data sources and business lines.
    - Run groups of rules and models alone, in parallel, or at different times (intraday, daily, weekly, monthly, etc.).

BIG DATA INGESTION, PREPARATION, INTEGRATION, AND ACCESS

As part of the source claims and non-claims data ingestion, preparation, and integration required for model development and execution to detect fraud, billions of rows are loaded to the Hadoop Distributed File System (HDFS) big data platform and are accessed using Hive protocol. SAS/ACCESS out-of-the-box interfaces provide enterprise data access from SAS Fraud Framework tools to data stored in HDFS. Hive provides a mechanism to access this data using a SQL-like language called HiveQL. Once data is loaded into a Hive table, it can be accessed from SAS as if it was a native data set or any other relational database table.

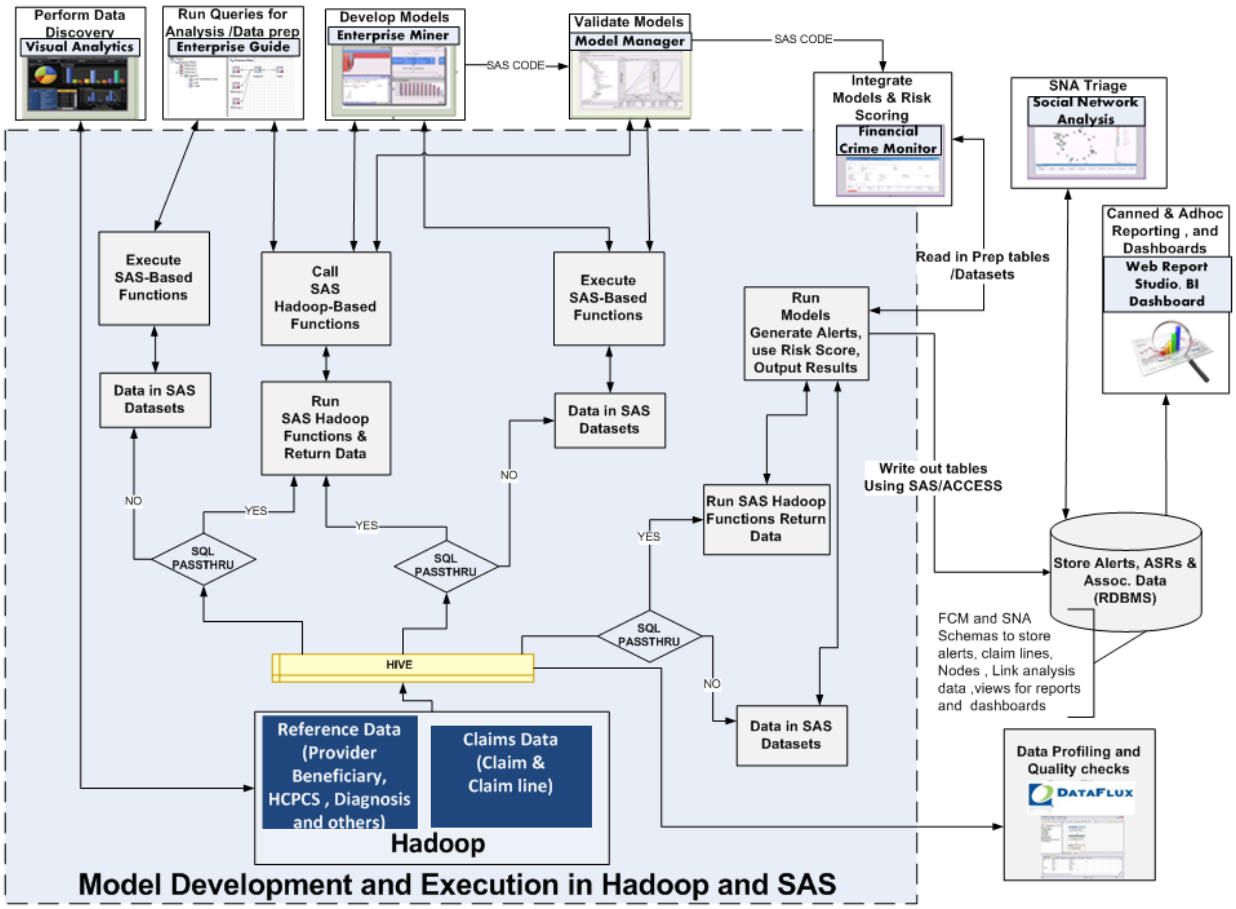

Figure 5. Big Data Ingestion, Integration and Access

Figure 5 shows the data ingestion, integration, and access flow for the SAS Fraud Framework set of tools for detecting fraud and abuse in Medicare. Some of the use cases are as follows:

- Source data for Model execution and generating alerts and provider profile: **Hadoop/Hive**
- Target database (DB) for writing alerts, actions, activities, leads, dispositions, and social network data: **RDBMS (for example, Oracle, Teradata, SQL Server, DB2)**
- Target DB for storing prep tables and intermediate processing tables: **SAS Datasets**

Some Design Considerations

✓ **SQL Pass-Through Facility in Hadoop**: SQL pass-through is recommended to use as much as possible when accessing large volume of data for model execution, analytics, and data discovery. The SQL pass-through facility uses SAS/ACCESS to connect to a RDBMS and to send statements directly to the DBMS for execution. As an alternative to the SAS/ACCESS LIBNAME statement, this facility lets you use the SQL syntax of your DBMS. It supports any SQL that is not ANSI-standard that DBMS supports. PROC SQL supports multiple connections to Hadoop. When modelers and other users use multiple simultaneous connections, it is a must to use an alias argument to identify the different connections. If you do not specify an alias, the default HADOOP alias is used. The example below explicitly specifies the default Hive port and schema.

```
proc sql;  connect to hadoop (user="myuser" pw="mypwd" server=hxpduped port=10000
schema=default);
```

✓ **Concurrent processing using Hive Server:** HiveServer is an optional service that allows a remote client to submit requests to Hive, using a variety of programming languages, and retrieve results. HiveServer cannot handle concurrent requests from more than one client. This is a limitation imposed by the Thrift interface that HiveServer exports, and can't be resolved by modifying the HiveServer code. HiveServer2 is a rewrite of

HiveServer that addresses these problems, starting with Hive 0.11.0. The SAS Fraud Framework is currently supported on SAS 9.3. SAS 9.3 supports HiveServer but not HiveServer2. As a result, one of the following options were considered to address this issue:

- **Option 1:** Work with SAS R&D to receive a 9.3 hot fix to support HiveServer2.
- **Option 2:** Upgrade to the next GA release of the SAS Fraud Framework, which is scheduled to be released on SAS 9.4 in April 2014. SAS 9.4 supports HiveServer2.

MODEL DEVELOPMENT

Model development should adapt to changing fraud schemes and the evolving healthcare environment. Flexible, scalable, and rapid technology modeling techniques are necessary to keep pace with the new and varying fraud schemes criminals employ to circumvent existing fraud prevention and detection methods. It is key that models should demonstrate the flexibility to add attributes quickly to identify and potentially prevent payment to fraudulent providers. Model development should accommodate a variety of model types to address multiple kinds of fraud schemes. Models can be built on one another in a continuum of sophistication, and have the ability to evolve from one type to another as the investigator and analytical lab teams collect more information to updates models.

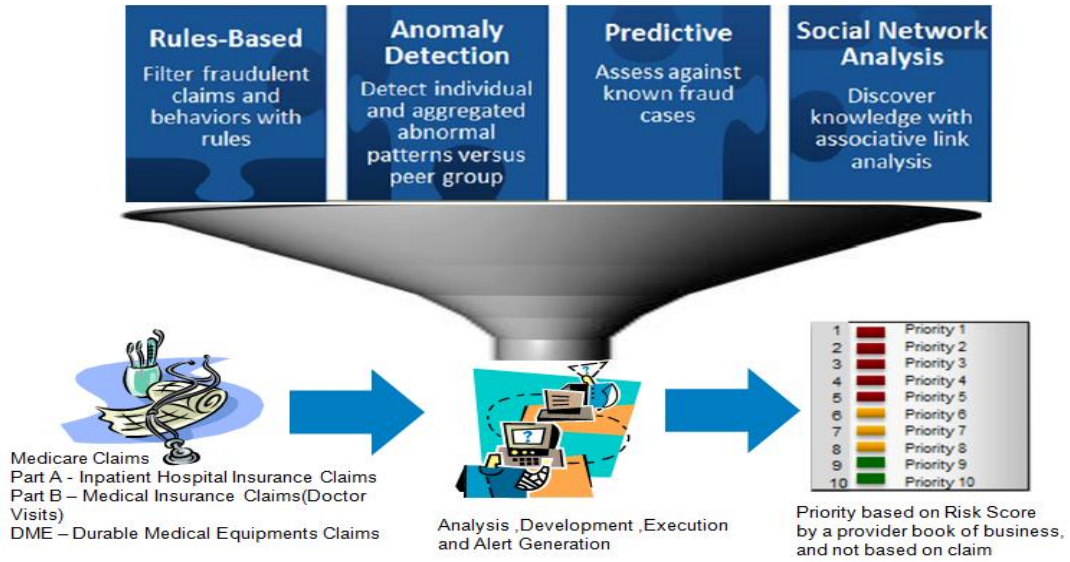

Figure 6. Model Development And Execution

Figure 6 shows four types of models that can be developed based on the need and business use case: rules-based, anomaly detection, predictive, and social network analysis.

Rules-based models

Rules-based models are based on known patterns of fraud. They are simple yet robust screens filtering all claims for known types of fraud and patterns of potentially fraudulent behavior.

Anomaly detection models

Sophisticated anomaly detection models define thresholds of acceptable behavior. They identify claims submission abnormalities by comparing an individual provider's behavior patterns through time and against aggregated patterns of a peer group. The complexities of medical claims mean that detecting and stopping fraud may require more sophisticated analyses than the rules-based models' simple "yes/no" decisions. Certain behaviors and characteristics that indicate potential fraud may also be indications of acceptable behavior. For example, if a provider bills for many more services than are normally performed by similar providers in a defined time period, the system can alert an investigator to inspect the claim prior to payment.

Predictive models

Development of advanced predictive models is based on past known fraud cases. Given the volume of fraud and the rapidly changing fraud environment, however, it can be challenging to find sufficient known cases with similar patterns, and models may need to start with limited information and develop or "learn" over time. The modeling team can implement complex predictive models leveraging the common characteristics of providers in known fraud cases.

Developing predictive models requires advanced analysis because a fraudulent claim may become apparent only when factors are considered in combination; whereas independently, those factors may not be suspicious.

Social network analysis models

Social network analysis models are built on providers that are associated with identified linkages among potentially fraudulent subjects. The ability to link providers through their social networks helps investigation teams and law enforcement partners unravel the complex relationships among fraudulent providers and between providers and beneficiaries (e.g., shared beneficiaries) and assess the risk level of these relationships.

BI AND REPORTING

Implementing an integrated and flexible BI and Reporting framework is crucial to help investigators, analytical lab members, business owners (management), law enforcement, and other end users to access data and interpret it to improve fraud and abuse outcomes using meaningful quality reports. Users can create custom reports ranging from high-level board reporting to extensive, detailed documents needed for supervisory oversight. Users can access custom, interactive dashboards on demand to gain critical information and reports in a visual interface. The solution also creates an audit record for management, examiners, or regulatory agencies that contains user identification, a time stamp, and the date when actions are performed. Interactive dashboards enable management to analyze operational performance of investigative functions and recognize trends to provide improved oversight and Governance of risk management practices. Some of the core reporting and BI areas are:

- **Operational reporting**
  - ✓ ***Efficiency***
    - Model monitoring & vulnerability management
    - Time to market a model that resulted in an actionable outcome
  - ✓ ***Performance***
    - Case actions, activities, and outcomes
    - Investigator workload assignment and performance
  - ✓ ***Return on Investment (ROI)***
    - Projected money saved from pre- and post-fraud detection.
  - ✓ ***Accuracy***
    - How many alerts were false positive vs. true positives?
- **Self-service and ad hoc reporting capabilities**
  - ✓ Ability to download data in Excel and manipulate as needed
  - ✓ Ability to save and share reports within investigator teams and analytical labs
- **Ease of use**
  - ✓ Seamless navigation from the case management system to reports and vice versa
  - ✓ Ability to drill down from alert summary reports to investigative claim lines

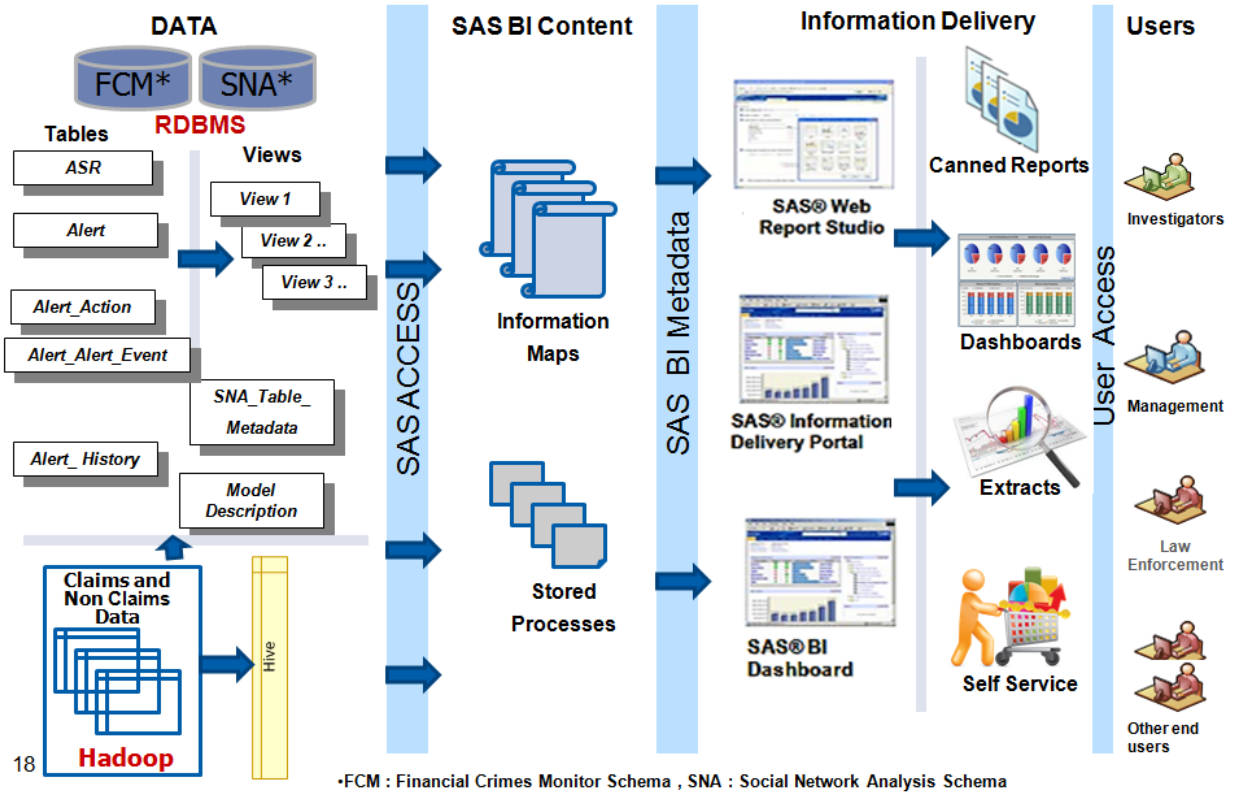

Figure 7. BI and Reporting Solution Architecture (Conceptual)

Figure 7 shows a beginning-to-end solution architecture for implementing a comprehensive, flexible, and scalable BI and reporting solution architecture using the SAS Enterprise business intelligence toolset, which is part of the SAS Fraud Framework.

SECURITY MODEL

With the increasing number of users and their multiple roles and responsibilities for detecting fraud and abuse, managing the environment is a topic of concern for IT from a security as well as a user experience point of view. Therefore, providing enhanced ways of controlling and configuring user roles and capabilities is critical to managing and securing the system. Implementing a custom security model is an essential part of a successful and secured fraud detection framework. Role-based access is defined based on user role, features, and functionalities required for using appropriate tools within the SAS Fraud Framework and accessing appropriate data sources. While permissions affect access to individual objects, roles control the availability of application features (such as certain buttons, plug-ins, and menu items in the case management user interface). For example, role memberships determine which user can view the disposition tab in the alert detail screen.

Some key points:

✓ Role:

- In general, roles do not protect data or metadata. Roles only control which features in a particular application are available to which users.
- An application feature that is under role-based management is called a capability. Each role provides multiple capabilities. A user or group can be in multiple roles.
- Not all applications have roles. Not all application features are under role management. Each application that supports roles provides a fixed set of capabilities.

✓ User Identity:

- In an authentication provider (for example, Lightweight Directory Access Protocol (LDAP)), the user has an account that can access the metadata server.
- In the SAS metadata, the user has a definition that includes a copy of the account ID with which the user accesses the metadata server. Coordination between these two realms establishes a unique SAS identity

for each user.

- Each SAS identity is based on a match between the following two values:
  - The account ID with which the user authenticates
  - The account ID that is listed in the user's metadata definition

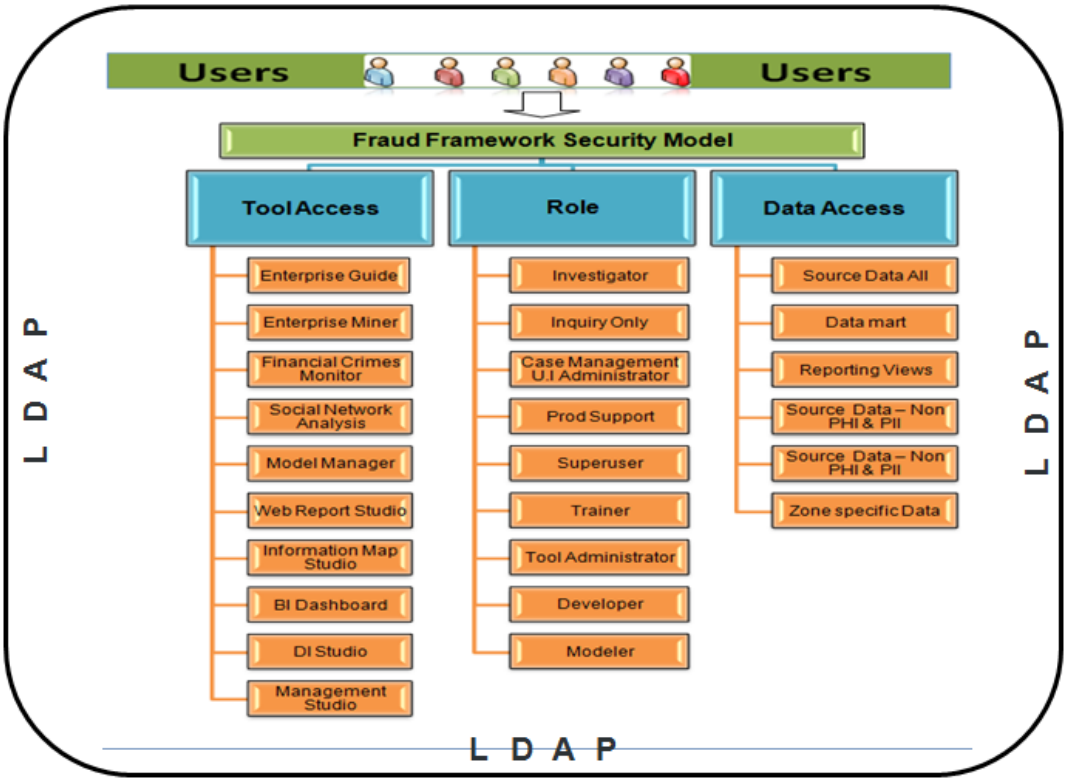

Figure 8. Security Model

As shown in Figure 8, user roles are defined based on the user function, required tool access, and authorized data access. LDAP protocol is used to define the base foundation user roles and groups.

FRAUD, WASTE, AND ABUSE (FWA) USER GROUP

An active and robust user community is essential to getting the most value from any solution. Identifying major areas of need, devising strategies to promote user participation in training, and bringing users together to share experiences and best practices in identifying and preventing fraud and Abuse is crucial to our success.

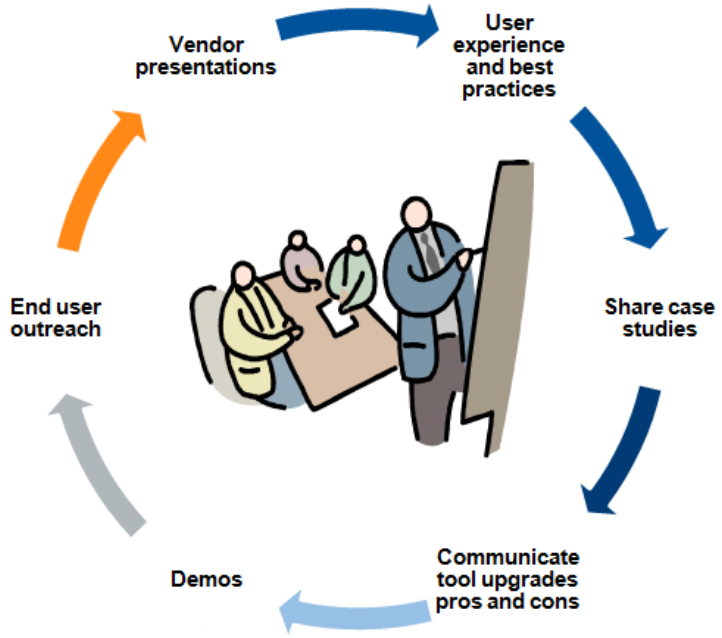

Figure 9. FWA User group

As shown in Figure 9, some of the core functions of the user group include:

- **User outreach**: Use and leverage reporting tools and various related applications, and tap into the under-utilized or non-utilized fraud framework tool to take full advantage of advanced analytic capabilities, including data mining and link analysis.
- **Share the User Experience and Best Practices**: Identify and promote major areas of need, devise strategies to promote user participation in training, and bring users together to share user experiences, best practices, naming standards, change management, and coding standards that are crucial to develop and deploy models quickly.
- **Share Industry Case Studies**: Invite guest speakers from healthcare to share challenges, experiences, and best practices in addressing healthcare fraud, waste, and abuse.
- **Share SAS Fraud Framework Tool Upgrades**: Present SAS Fraud Framework new version demos, pros and cons, upgrade strategy, and upgrade plans.
- **Project Demos**: Present an overview of solution architectures to make sure users understand how reporting, case management, and vulnerabilities management work from beginning to end in a typical implementation.
- **Vendor Participation**: Vendor representatives have an opportunity to present best practices, tips and tricks, and future technological innovations.

TRAINING AND USER OUTREACH

Training and user enablement play a key role in the effective and efficient use of any system, and proactively keep user communities up to date on fraud and abuse processes, best practices, tool features, and functionalities. The following are some user outreach and enablement activities.

Training

Tailor to Users: Train users how to use the tool with their own data, how to use and interpret the data, and what actions to take. Highlight specific features and functionalities of the tool, tips and tricks, best practices for achieving optimal performance, security model, VPN profiles, how to access the SAS Fraud Framework set of tools from Citrix, folder structures, data libraries, change management, and more.

Train the Trainers: Train users to train their colleagues regarding how to address day-to-day operational challenges such as scheduling reports, saving report outputs, and downloading investigative claim lines in Excel or .csv.

Use More Training Options: Offer classroom, online (Webinar), and self-paced training videos.

User outreach

Monitor System Usage: Know how users and groups use the system and to what degree. Monitor usage and usage patterns and tailor performance tuning and queries to meet user needs.

Electronic User Forum: Track and catalog questions received by administrators and the helpdesk. Publish FAQS and tool usage best practices, such as: Social network analysis tips and tricks, Top 3 filter conditions when viewing Alert summary, optimal drill-through paths - Summary to Alert, and from Alert to investigative claim lines.

User Surveys and Interviews:

- ✓ Conduct pre-project customer surveys and interviews to better understand upcoming user requirements and pain points.
- ✓ Conduct frequent post-project surveys to gauge user experience in using the tool.
- ✓ Examine and measure the effectiveness of every model and share success stories and lessons learned.

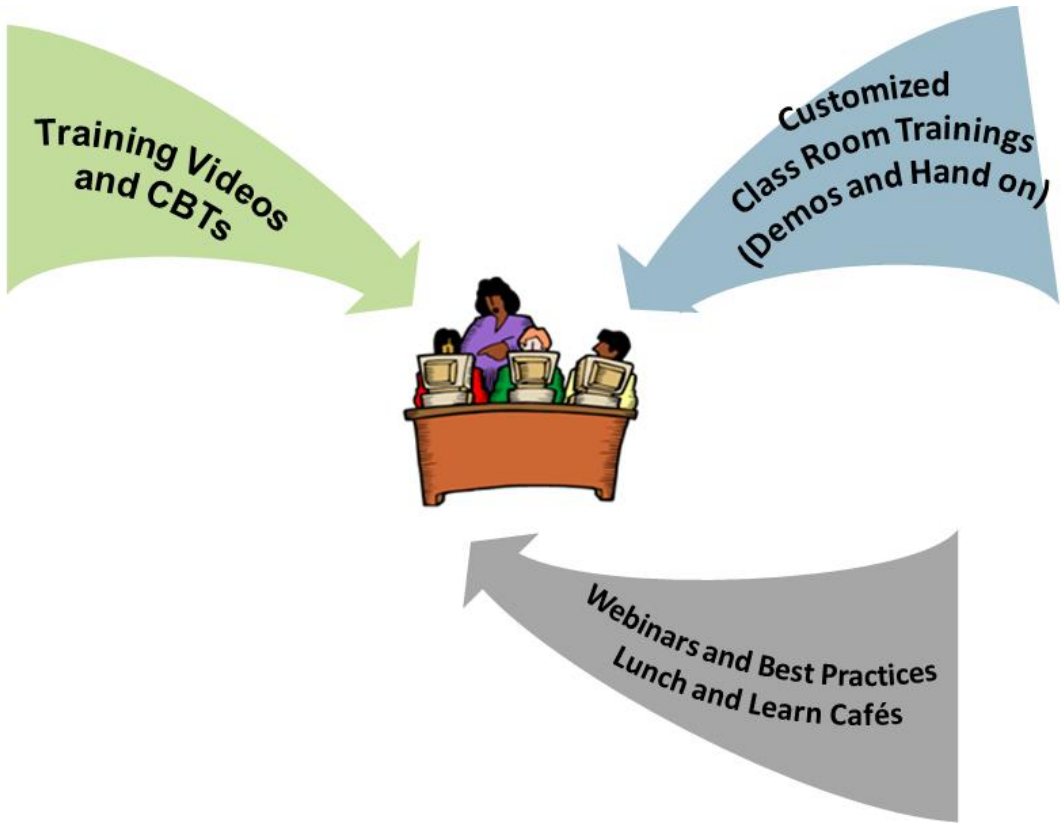

Figure 10. Training options

Figure 10 shows different training options, such as classroom, online (Webinar), self-paced training videos, computer-based training (CBT), and lunch and learn cafés. One or more of these training methods can be used to increase user engagement and enabling.

ANALYTICAL LAB DIVISION

The analytical lab division is a dedicated team of statisticians, data scientists, power users, researchers, and Medicare SMEs. Their primary responsibilities are:

- Providing statistical and data analysis for vulnerabilities management and fraud schemes
- Identifying emerging fraud trends through data mining and other advanced analytical techniques
- Leading model development and alert prioritization for Fraud Prevention
- Prioritizing vulnerabilities for predictive modeling and approving promotion of effective models and enhancements to production

- Overseeing rigorous phased testing to confirm new or enhanced models' effectiveness
- Producing operational reports to calculate ROI on pre- and post-fraud detection

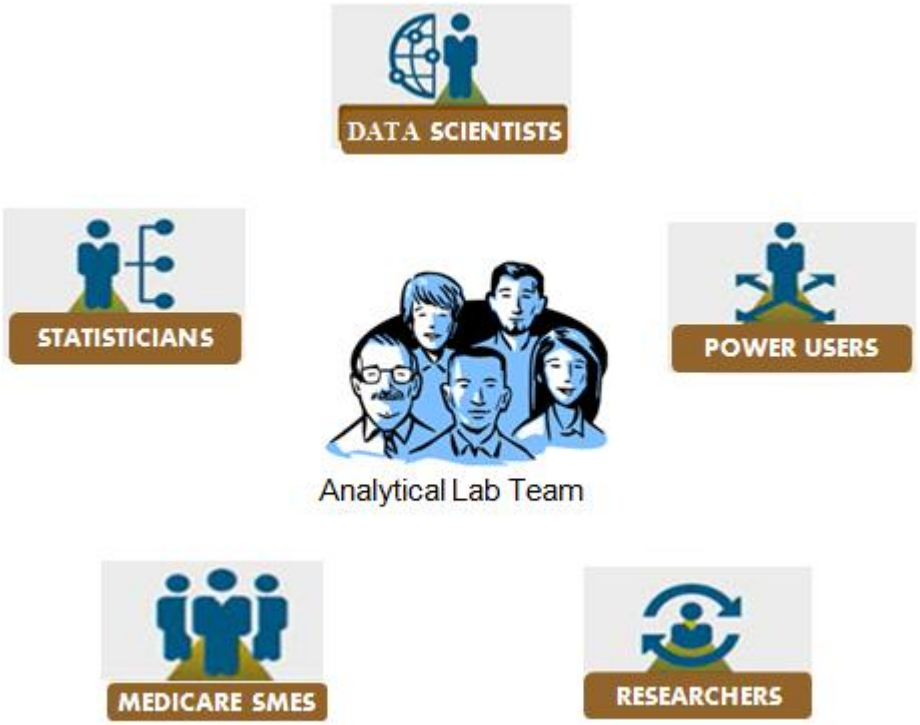

Figure 11. Analytical Lab Team

CASE MANAGEMENT SYSTEM

Case management is a key component of the Fraud and Abuse Framework, and is garnering attention for its potential to combine intelligence from all disparate fraud systems and departments into a single repository to more effectively prevent fraud and abuse, meet regulatory compliance mandates, and reduce costs. Case Management provides a structured environment to establish and enforce best practices across the organization, linking present day siloed systems into an enterprise wide perspective. With this unified solution, investigators can manage case workflows, add comments and attach documentation, and record exposure and losses. Its holistic perspective opens communication between departments and clarifies issues that would be missed with today's disparate processes and tools. Case Management significantly reduces the time and effort of investigating fraud schemes. For example, recently CMS stated that Fraud Prevention systems decrease investigation time from days and weeks to a matter of hours. Some of the key features of an enterprise case management system are:

- ***High-level oversight***: More than a simple dashboard to track and monitor individual cases, a best-in-class case management tool unifies multiple source systems into a single enterprise-wide view.
- ***Unified repository of case management information***: Integrate and standardize data from multiple systems and business units, such as operational systems, databases, and fraud detection systems. Data quality rules are applied consistently across all data sources and platforms to deliver a unified, accurate view across the organization. Structured and unstructured data can be linked for analysis and review.
- ***Efficient workspace for managing cases***: Cases flagged for review/action can be automatically assigned to an investigator based on the type or category of the incident. When an investigator logs into the system, he or she is presented with a list of tasks and a structured environment in which to manage them. Information is entered in online forms that are dynamically linked to custom workflows. The investigator can then:
  - ✓ See active and pending tasks, displaying details by case.
  - ✓ Add freeform comments and attach documentation (including digital media, such as videos) to the case.
  - ✓ See cases and incidents that may currently or have been previously worked in another department.
  - ✓ Maintain a complete audit trail of actions taken on a case and who performed those actions.

- ✓ Generate summary and detail reports on demand.

- ***Coordinated best practices***: Investigators need a central workspace to manage a case from initiation to resolution and preserve the information for later research and continuous process improvement.
- ***Correlation across departments***: The system can reveal commonalities among thousands of cases, identifying potentially suspicious activities that the human eye would miss.
- ***Automated, tailored processes***: Workflows must be customizable to reflect the organization's unique structure and policies.

CONCLUSION

The management and control of improper payments and fraud require an iterative process of constant, consistent monitoring. Each agency's unique culture and business processes require the implementation of a fraud, waste, and abuse framework that is flexible to meet both the variety of internal business processes and the ever-changing ways that fraudsters try to exploit those processes. There are various approaches to counteract fraud, waste, abuse, and improper payments, ranging from step-by-step individual solutions implemented by agencies to address targeted challenges, to an enterprise-wide approach in which agencies implement a comprehensive solution package for solving a variety of fraud challenges across the organization. No matter where the agency is in developing an anti-fraud strategy, leaders can identify and implement an FWA framework that allows them to use and augment current infrastructure resources, and refine and monitor existing organizational processes to stop fraud, waste, and abuse before money is lost.

The National Healthcare Anti-fraud Association (NHCAA) cites an average of 3 percent (at the low end) and 10 percent (at the high end) of healthcare spending is lost due to fraud. That's between $67 billion and $230 billion lost to fraud, waste, or abuse each year, or between $184 million and $630 million lost each day. This number is expected to increase every year as healthcare costs rise. The magnitude of potential fraud and abuse savings is such that as more payers recognize the need for an FWA framework that comprises components and toolsets for optimal, innovative, and exceptional fraud and abuse detection capabilities, those with antiquated fraud management practices will be at a significant competitive disadvantage.

Based on a report published by the CMS Program Integrity group to Congress in December 2013, "Within the first year of implementing a fraud prevention system, CMS stopped, prevented, or identified an estimated $115.4 million in payments. Although it is not typical for information technology investments to achieve a positive return on investment within just 12 months of implementation, the system produced an estimated $3 for every $1 spent in its very first year and also generated leads for 536 new investigations by CMS's program integrity contractors and augmented information for 511 pre-existing investigations. These savings are expected to grow every year." Implementing a comprehensive fraud, waste, and abuse framework had helped agencies like CMS be well ahead of the statutory implementation schedule, which calls for phasing in the technology in the 10 highest fraud states in the Medicare Fee-For-Service program by July 1, 2011, and nationwide by 2014.

We highly recommend that agencies and companies invest in a fraud, waste, and abuse framework. A phased approach can be taken to implement all or a combination of the components listed in this paper; either way, we expect the investigative teams will be well-rewarded. It is essential to invest in a framework to prevent claims fraud and abuse, and stem the current epidemic of financial losses. This framework complements a broad array of existing anti-fraud activities carried out by companies and agencies. We strongly believe this paper provides IT leaders a clear path for resolving issues from the simple to the incredibly complex through a measured and scalable approach for delivering value for a fraud, waste, and abuse programs by providing deep insights to support evidence-based investigations.

REFERENCES

- Health care fraud, waste and abuse statistics available at http://www.stopmedicarefraud.gov/newsroom/
- Fraud and Abuse fact sheet available at http://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/downloads/Fraud_and_Abuse.pdf
- Report to Congress Fraud Prevention System First Implementation Year 2012 available at http://www.stopmedicarefraud.gov/fraud-rtc12142012.pdf
- The National Healthcare Anti-fraud Association (NHCAA), "Anti-Fraud Resource, Consumer Info & Action," available at http://www.nhcaa.org/eweb/DynamicPage.aspx?webcode=anti_fraud_resource_centr&wpscode=ConsumerAndActionInf

- Perspective on Cost Containment: Fraud and Improper Payments by SAS featuring Marc Pierce, Stone gate Advisors, LLC, Alok Verma, Stone gate Advisors, LLC Julie Malida, SAS, Greg R. McFaul, SAS
- Protecting the Enterprise: Enterprise Fraud Strategy – Vision and Reality, by Fraud Management Institute June 2010
- The SAS® Fraud Framework for Health Care product brief by the SAS Institute
- Enterprise-wide Fraud Management White paper by the SAS Institute
- Bringing the Power of SAS® to Hadoop White paper by the SAS Institute

ACKNOWLEDGMENTS

I'm especially grateful to my colleagues **Wayne Parker** (Technical Advisor – Health IT), **Amir Drusbosky** (Program Manager – FPS) and **John Thomas** (Technical Director, Healthcare Systems Management) at Northrop Grumman for mentoring , advising and guiding me through the process. Finally, I want to thank my fellow SAS users in the community, including those on the SAS Institute R&D, product management, **Stacey Jenks** and **Gary Shore** from the SAS Federal team, and my SGF 2014 point of contact **Sara Jones**, who are always at the ready to answer my questions via email, phone, or Twitter.

CONTACT INFORMATION

Your comments and questions are valued and encouraged. Contact the author at:

Name: Vivek Sethunatesan
Designation: Technical Advisor – Health IT
Organization: Northrop Grumman Information Systems
Address: 2810 Lord Baltimore Drive
City, State ZIP: Baltimore, MD 21244
Work Phone: 240-755-7625, 410-782-5436
Email: Vivekanandan.sethunatesan@ngc.com
Viveksethunatesan@gmail.com
Web: http://www.northropgrumman.com

LinkedIn: www.linkedin.com/pub/vivek-sethunatesan-a-k-a-vivek-seth/7/358/ab8/
Twitter : vivekseth@TDWI_DC_Buzz