Application Brief

Caught on Computer

The Healthcare Industry Fraud Problem

A Houston physician's patients received the best in medical care—state-of-the-art surgical procedures, brand-name drugs, home-health visits, outpatient services, physical therapy, and the highest-quality medical supplies. Another doctor's dedication often kept him on the job more than 18 hours a day. And one clinic often arranged for specially equipped vans or ambulances to pick up nursing home patients or others who were unable to arrange their own transportation, even when a much-cheaper taxi would have sufficed.

As the state Medicaid claims processors reviewed the bills submitted by these clinics and doctors, everything seemed to be in order. But the manual review process failed to catch several important details, including the fact that the Houston physician whose name appeared on the Medicaid forms had been dead for months.

Remarkably, these are not fictitious anecdotes[1] but examples of fraud cases that have been detected using the ITC fraud detection system. The offending Houston clinic agreed to pay the state of Texas several million dollars for improper billing of services, and settlements were negotiated with the other providers. Some cases were also considered for referral to the district attorney's office for criminal prosecution.

Every year in the United States, fraud and abuse deplete healthcare coffers of an estimated $100 billion—approximately one dollar of every 10 distributed[2]—in fake claims, overbilling, unnecessary procedures, and a host of other illegal schemes perpetrated by both providers and recipients. Such fraudulent activities lead to higher overall costs for healthcare and, in many cases, exhaust the government's financial resources to the point where the program cannot satisfy the medical needs of low-income families, the elderly, the disabled, and others who critically depend upon Medicaid services.

So why has it taken so long to fix the problem? Consider the high transaction volumes. For example, the state of Texas annually processes more than 26 million Medicaid claims submitted from 60,000 providers. Healthcare claims can include a complex mix of services and multiple providers, and the data may be incomplete or fragmented. Then factor in the resourcefulness of the swindlers. Many schemes are impossible to detect unless large amounts of data can be scrutinized over time. Creative criminals change their scams, so an effective fraud management solution must be able to find more than predefined patterns.

Although the government has invested millions of dollars in Medicaid information technology, most funds have gone to streamline claims processing or to improve eligibility determination. Only recently, as the real costs of fraud have become painfully clear, has the focus shifted to investigating and implementing fraud detection solutions. Likewise, it is important to note, only in the past few years have hardware and software technologies advanced sufficiently to handle the tremendous volume of Medicaid claims data and to solve the complexities of the fraud detection problem.

The manual review process failed to catch several important details, including the fact that the Houston physician whose name appeared on the Medicaid forms had been dead for months.

SGI™ Systems Help Stop Medicaid Fraud

At the State of Texas Health and Human Services Commission (HHSC), Medicaid fraud once unjustly claimed millions of taxpayer dollars and countless agency personnel resources. Today, SGI technology and fraud management application software from SGI's application provider, Intelligent Technologies Corporation, are helping Texas protect its revenues by targeting fraudulent providers and improving agency productivity.

The Texas Comptrollers Office estimated that in its first year of operation the system identified more than $50 million in questionable Medicaid payments. Recouping those dollars would yield a potential return on investment of 25:1. Rescued funds can be used to help reduce the state's overall healthcare costs and to deliver more medical services to the people who need them.

Intelligent Technologies Corporation (ITC) developed the fraud management system in a project done with the state of Texas. Working with SGI, Electronic Data Systems (EDS), and HNC Software Solutions, ITC extended the system to a fully operational pilot that was deployed statewide in late 1997. The fraud management solution, running on an SGI™ Origin™ 2000 server, utilizes multiple detection technologies that increase system accuracy and efficiency, even as transaction volumes increase. This hybrid, highly scalable design makes the system applicable for fraud prevention in other fields—such as insurance and financial services—in both the public and the private sectors.

The State of Texas Medicaid Fraud Detection System

State officials in Texas suspect that total losses in their state could be as high as $850 million per year. In 1995, the Texas Comptroller at that time, John Sharp, initiated the Medicaid Fraud Detection project to help officials quantify the state's abuse problem and to investigate potential solutions. As part of this effort, Sharp's office employed ITC to test the feasibility of using a system that incorporates neural network technology—technology that ITC's founders helped successfully implement at Visa, where the system was able to automatically identify about 45% of the fraudulent cases.[3] The goal was to develop a demonstration project that would test the compatibility of ITC's system with the unique complexities of Medicaid claims.

The first version of the Medicaid Fraud and Abuse Detection System (MFADS) was developed over the course of a nine-month feasibility study. During this phase, ITC worked with the Comptroller's Office to look at data from a small number of Texas counties and three databases, including eligibility, claims history, and vendor drugs. The test also considered the applicability of combining neural networks with related technologies such as algorithms (filters), fuzzy logic, and statistical analysis to improve accuracy and enhance detection.

At the completion of the prototype phase in August 1996, an independent review showed that performance of the ITC detection system exceeded original expectations. Comparing results of the MFADS against the existing Surveillance Utilization Review Subsystem (SURS), a program mandated by the federal government, the investigators determined that the innovative technology underlying the MFADS spotlighted 39% of the sample claims that warranted further investigation, while SURS only detected problems with 14% of the claims. The positive results of this study led to an extension of the contract with ITC for development of a fully operational prototype. The system was to incorporate an enlarged data set with more counties and additional databases and be turned over to the Health and Human Services commission, the agency that oversees the Texas Medicaid program.

The Technologies

Neural networks: *Neural network technology, a form of data mining, is fashioned to mimic the human brain's learning methods. A neural network accumulates knowledge over time, learning by example and developing its own expertise to solve extremely complex problems. Inherently nonlinear, neural networks are ideal for solving real-world problems. Joe Brown, ITC president and chief executive officer, describes its relevance to fraud management: "Learning by example is critical when dealing with fraud—criminal behavior is dynamic and often one step ahead of the law. So many systems may not work because they follow a set of prewritten rules and assume we already know the answer. Neural networks simply outperform other techniques because they more exactly model the real-world problem."*

Filters (algorithms, expert rules): *Filters allow existing policies to be explicitly represented and enforced. Filters define a set of known characteristics—for example, typical fraud scenarios—for which the detection engine should search. The ITC solution includes more than 200 fraud filters targeted at a wide range of healthcare schemes. Examples include time contradictions, services unbundling, home healthcare, dental, ambulance, inpatient hospital, and outpatient hospital.*

Statistical analysis: *Most existing Medicaid fraud detection systems rely primarily on statistical analysis to detect unexpected deviations from norms. Statistical analysis is critical to any fraud detection system, but used alone it may not pick up those unexpected deviations that remain within targets.*

Fuzzy logic: *Differing from classical logical systems, fuzzy logic-based solutions use reasoning methods that are approximate rather than exact. Fuzzy logic incorporates techniques for representing and inferring information from knowledge that is incomplete or imprecise. In the Medicaid system, for example, fuzzy logic allows consideration of less-than-perfect data derived from submitted claims forms. A system that only accepts precisely formatted data—exact matches—potentially misses critical puzzle pieces.*

Creative criminals change their scams, so an effective fraud management solution must be able to find more than predefined patterns.

The Medicaid Fraud and Abuse Detection System

The development phase of the program ran from September 1996 to August 1997. The project data set was extended to evaluate 4.8 million claims, 10.2 million details, and 13,699 providers in 15 counties. The program was also enhanced to incorporate additional features and new fraud detection filters to be able to scrutinize the full breadth of provider types. The results astounded investigators. By retraining data models over the course of the project, the program achieved a hit rate [for locating suspect claims] that began at 39% and rose to an impressive 72% during the last months of the development phase. Simultaneously, the false alarm rate was held at a constant 25%.

Based on the system's success, the Texas Legislature called for statewide deployment, beginning in December 1997. Shortly after implementation, the Health and Human Services Commission noted in a status report, "In just two months, utilizing only three out of the 22 existing algorithms [developed by ITC, the system] has produced 244 suspects and identified $623,096 in overpayments in a 53-county database. Each of the three algorithms used in Phase I produced suspects and identified overpayment dollars that would not have otherwise been identified by existing Medicaid automated systems."[4] The report also concluded that the system identified dollars that, if collected, would recover 85% of system operation costs for that period. Additionally, staff productivity improvements were noted, with percentages ranging from 68 to 89%.

Solution Components

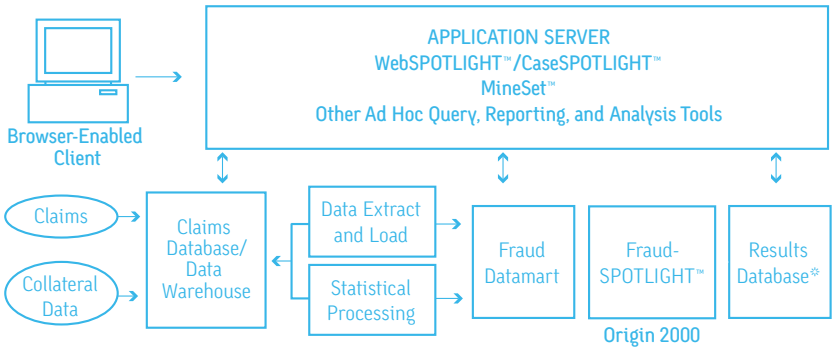
The Medicaid fraud management system is based on integrated products from ITC, Oracle, and SGI. Key features of the integrated MFADS solution include:

- Support for multiple data sources
- A detection engine based on advanced statistical and data modeling techniques
- Automated detection
- Priority-ranked suspect lists
- Web-based browser "drilldown" (built on the relational database) that lets investigators easily navigate through layers of supporting data and statistics
- Integrated case tracking with audit trail recorded for each case
- Data warehouse architecture optimized for healthcare applications
- Minimal technical complexity to encourage use and enhance investigator productivity

While most fraud systems emphasize a single detection approach, the ITC solution combines multiple approaches for better detection and better defense. ITC's Brown explains: "SGI is an optimum platform for the ITC solution. Origin 2000 provides superior scalability and performance to accommodate large and growing databases and SPOTLIGHT's need for floating-point capability. Additionally, SGI MineSet is an industry-leading visualization tool that supports quicker detection of fraudulent behavior. This technological advantage is further underscored by SGI's corporate focus on the fraud detection market."

The system, with proven fraud detection capabilities, helps the state government ensure that taxpayers' dollars are used as intended.

Solution Architecture



*Identified suspect activity, fraud-risk scores, and score explanations

The solution architecture integrates the following product components:

From ITC:
FraudSPOTLIGHT. This detection engine combines statistical techniques, fraud filters, data matching, and advanced modeling technologies (including neural networks and fuzzy logic) to uncover complex patterns of healthcare fraud. The modeling technologies highly leverage the floating point capabilities of Origin 2000.

WebSPOTLIGHT. An intuitive user interface, WebSPOTLIGHT lets users directly access the data warehouse from any standard desktop computer. It operates through a standard Web browser such as Netscape Navigator® or Microsoft® Internet Explorer.

CaseSPOTLIGHT. CaseSPOTLIGHT helps investigators manage the investigation process, providing seamless access to suspect lists and open cases against suspects. Using it, processors can more easily track cases and execute auditing tasks.

From Oracle:
Oracle8™. This highly scalable relational database supports extremely large databases. It provides table and index partitioning features critical to data warehousing applications; parallel DML for enhanced operations on large tables; enforced and deferred constraints that save validation time and enhance operational concurrency; and data warehouse-class backup and recovery facilities.

From SGI:
MineSet. The SGI data mining and visualization application, integrated with the ITC SPOTLIGHT solution, enables faster insight from vast amounts of data. MineSet uses 3D visualization tools to help investigators quickly identify key trends and critical patterns. Users view data relationships in fresh ways to more easily spot fraud, abuse, and waste—problems that might otherwise go undetected without sophisticated visualization capabilities.

Origin 2000. The SGI ccNUMA integrated system performance and scalability enable the CPU performance, memory capacity, and I/O bandwidth that are essential to this extremely data-intensive application. Origin 2000 servers scale incrementally in both CPU power and throughput. The balanced-performance capabilities of the SGI server architecture also made it possible for ITC to optimize fraud filters to run faster on Origin 2000 than would be achievable on any other platform.

The Fraud Detection System Results and Benefits

The MFADS provides a cost-effective solution for the state, even as Medicaid program requirements expand. The system is able to manage increasingly large amounts of data and is highly extensible and scalable within its initial configuration. Effective fraud detection requires growing sets of data as new years and databases are added. In Texas, for example, 13 separate databases are integrated to enhance the fraud detection process. This incremental growth can be accommodated by the SPOTLIGHT and Origin 2000 solution without replacing the initial investment.

In terms of productivity enhancements, the system offers major improvements over previous claims analysis. As one example, investigators now enjoy a five-second or less response time to standard queries against a data array of 1.2TB.

The Wall Street Journal reported system results as follows: "Since the first of the year, the Health and Human Services Commission has used special 'smart technology' software, known as the Medicaid Fraud and Abuse Detection System, to spot possible fraudulent payments. Using the system, developed by Austin-based Intelligent Technologies Corp., the agency in the 1998 fiscal year recovered $97 million in improperly paid Medicaid funds, compared with $19 million in 1997."[5]

The system, with proven fraud detection capabilities, helps the state government ensure that taxpayers' dollars are used as intended. "ITC's smart bomb technology will make a dramatic difference in state government's effort to make sure Medicaid dollars are used effectively and efficiently," comments Sharp, former Texas State Comptroller, on the success of the team effort. "We believe it will set the standard for using limited resources to deal with a growing volume of transactions."

For more information, visit the following sites:
www.itctx.com
www.sgi.com

Footnotes:

[1] "Computer finds Medicaid fraud," Austin American-Statesman, December 17, 1997; "Computer finds suspicious billing in Texas Medicaid," Houston Chronicle, December 15, 1997.

[2] The U.S. GAO estimates that 10% of healthcare costs are lost due to waste, fraud, and abuse. The Inspector General's estimate was 12% (June 1997).

[3] American Banker Magazine, January 21, 1994

[4] From the ITC "Intelligent Fact Sheet" summarizing the MFADS project

[5] The Wall Street Journal, Wednesday, December 9, 1998

Corporate Office
1600 Amphitheatre Pkwy.
Mountain View, CA 94043
(650) 960-1980
www.sgi.com

North America 1(800) 800-7441
Latin America 1(650) 933-4637
Europe (44) 118.925.75.00
Japan (81) 3.5488.1811
Asia Pacific (65) 771.0290

2307 (7/99) J10154