



# HEALTH CARE FRAUD REPORT



Reproduced with permission from Health Care Fraud Report, 14 HFRA 674 , 08/11/2010. Copyright © 2010 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

## Predictive Modeling, Analytics Expanding Fraud-Fighting Toolkit for Regulators

**R**egulators and law enforcement are expanding their use of new health care fraud-fighting technologies such as predictive modeling and analytical frameworks, allowing for real-time analysis of Medicare and Medicaid transactions, industry experts and government officials told BNA.

Predictive modeling and analytics involve data-mining large amounts of information and then building models of expected behavior. In a Medicare setting, for example, individual models can be created from information including health records, pharmacy use data, and prior health care claims, and then compared against incoming claims. When a claim deviates from the expected model, the system can flag it for further review.

The Dartmouth Atlas Project, which has been analyzing the distribution and consumption of medical care in the United States for the past 20 years, has utilized modeling and data-mining software from SAS, a provider of business analytics and business software based in Cary, N.C., to look for discrepancies in Medicare spending. The software can analyze large amounts of health care information, looking for patterns and models in Medicare claims data. Over the course of the Atlas Project, SAS software has helped lead to several hospital fraud investigations after identifying suspicious activity, according to an SAS white paper.

The Department of Health and Human Services has also used SAS software, and renewed a contract with SAS for three years in April 2009. HHS uses SAS software to fight Medicare fraud, waste, and abuse, provide disease surveillance information, and maintain food and drug safety, among other goals. SAS software is used throughout HHS, including in the Centers for Medicare & Medicaid Services.

Predictive modeling systems have been in use by the financial services industry for many years, and have been used to prevent credit card fraud in real-time settings.

For example, Bailey Spencer, a federal civilian sales manager with SAS, told BNA about getting blocked from buying a TV at an out-of-town Best Buy until he identified himself on the phone.

Spencer said that his trip to Buffalo, where he bought the TV, had been outside of his normal behavior, hence the phone call at the point of sale. "It's all about behavioral analytics, applying advanced analytics to identify potential fraud," he said.

**Medicare and Fraud Analytics.** The work of the Recovery Accountability and Transparency Board (RATB) is another example of technology being used by regulators in the fight against health care fraud. The RATB is currently involved in a pilot program with CMS that involves analyzing Medicare transactions with a privately-developed fraud mapping application. The RATB was created by the American Recovery and Reinvestment Act of 2009 to provide transparency for stimulus funding and prevent any associated fraud (14 HFRA 498, 6/16/10).

The pilot program was announced June 18 in a White House blog post by Peter Orszag, former director of the Office of Management and Budget.

"The RATB has deployed a cutting-edge fraud mapping tool that leverages the latest technologies in data capture and analytics to identify potential fraud and error," Orszag said in the blog post. He emphasized that the tool would be able to gather and analyze large amounts of information in real time and identify possible fraud, waste or abuse.

**“We can go into an in-depth analysis of the fund recipient. You might be as clean as a whistle, but you might have people within your company who have a criminal record. We’re able to check all the risks associated with the principals of a company.”**

DOUGLAS HASSEBROCK

ASSISTANT DIRECTOR FOR INVESTIGATIONS  
RECOVERY ACCOUNTABILITY AND TRANSPARENCY BOARD

“Medicare has received recovery money. We’re looking at both funding CMS received from ARRA and other funding they have, and focusing on the risks posed by the recipients of the funding,” Douglas Hassebrock, assistant director for investigations at the RATB, told BNA.

The fraud mapping application was developed in conjunction with several private firms, Hassebrock said, including Palantir, Regulatory Data Corp. (RDC), Dun & Bradstreet, HMS Inc., and Grant Thornton.

RDC, a data aggregator, provides the fraud tool with a constantly updated stream of data from a custodial public source database on risk. The information is then filtered through Palantir’s analytic platform to identify suspected fraud.

All recipients of federal money, including health care professionals, are required to have a DUNS number, a nine-digit identifier from Dun & Bradstreet that allows the federal government to track monetary distributions. This number allows the RATB fraud analytics tool to look at the recipients of CMS funding in much the same way that a bank looks at loan recipients, Hassebrock said.

“We can go into an in-depth analysis of the fund recipient. You might be as clean as a whistle, but you might have people within your company who have a criminal record. We’re able to check all the risks associated with the principals of a company,” Hassebrock said. Hassebrock said that a full analysis takes a day to a few days, based on the complexity of the case.

The fraud analytics tool geo-codes everything, Hassebrock said, meaning that all information is placed on a map for easy viewing.

“There is no one-stop solution. We can’t validate the results we get, CMS will have to do that. We’re a lead factory, designed to focus CMS fraud-fighting efforts,” Hassebrock said. The pilot program is not expected to be completed before early September, Hassebrock said.

“As we’re processing the data CMS gives us, we’ll provide them with periodic updates. We won’t hold up results and wait for a big reveal,” he said.

If CMS likes the results from the pilot program, they might procure their own system, based on the RATB model, Hassebrock said.

**Predictive Modeling Systems.** Predictive modeling software, which is used to detect suspicious patterns and behaviors, is capable of handling the massive amount of

information associated with CMS transactions, Jeff Mudd, a federal sales director with SAS, told BNA.

“It’s time for the implementation discussion. The analytic technology is available now to detect and score fraud in real time as well as scale to massive amounts of data,” Mudd said.

Mudd said that analytics software can help stem the tide of health care fraud by detecting the fraud and then by focusing subsequent investigations by allocating resources more efficiently, among other steps.

“There’s been a tremendous uptick in public perception of health care fraud. Fundamentally, we need to move away from the pay and chase model. You need to stop fraud at the point of sale. What can’t happen is the delay of legitimate payments,” Mudd said.

Mudd said that the error rates for SAS software were extremely low.

**Social Network Analysis.** A new fraud fighting tool, known as social network analysis, is starting to gain interest within the health care community, Julie Malida, a principal for health care fraud with SAS told BNA.

“Social network analysis, which is also called link analysis, involves building statistically significant links between people, then running the links back through predictive modeling and anomaly detection systems,” Malida said.

Organized crime and collusion are growing trends within health care fraud, Malida said, and link analysis can fully detect the disparate relationships that often occur within crime rings.

“The largest health plans are beginning to understand link analysis and the use of social networking, and it’s definitely on their radar screens. Overall, the interest in fighting fraud has really ramped up since the passage of the Patient Protection and Affordable Care Act [Pub. L. No. 111-148],” Malida said.

**Constant Fine-Tuning.** An important component of a successful analytical model is the ability to change, Spencer said.

“You’re always looking for the champion model, the model that has the highest chance of avoiding false positives. You keep checking and adjusting the model. It’s about constant fine-tuning,” Spencer said.

The fine-tuning results in investigators pursuing fewer false positives and improved fraud identification rates, he said.

“Fraudsters are extremely dynamic, constantly changing their strategies, so analytical models need to keep up,” Spencer said.

**Congressional Activity.** Of late, there has been increased interest in fraud detection software from Congress, including several bills that specifically call for the adoption of software to help rein in Medicare and Medicaid fraud.

One such bill, H.R. 5546, would require CMS to implement a prepayment review prevention system. Sponsored by Rep. Peter Roskam (R-Ill.), the bill would require the system to analyze CMS claims in near real time, flagging any suspicious activity for further review and investigation. All flagged claims would be prevented from being paid until after review.

“Predictive modeling ‘scores’ a claim to identify claims that have a high probability of fraud. A predictive model creates an estimated score on claims using historical data. That estimate is then applied to new

---

claims that are submitted. The predictive model is always evolving, improving and adapting to provider and patient behavior,” Roskam said in June 15 testimony before a hearing of the House Ways and Means Subcommittee on Health focused on Medicare fraud (14 HFRA 498, 6/16/10).

The AARP endorsed Roskam’s bill on July 27, along with two other Medicare fraud-fighting bills. A predic-

tive modeling program for Medicare fraud was added to the Senate version of H.R. 5297, the Small Business Jobs Act (*see related item in the Federal News section*). The bill was sent to the Senate Committee on Finance on Aug. 5 with instructions to report the bill back to the Senate with the addition of an amendment. The Senate is on recess until Sept. 13.

By JAMES SWANN