SYNOPSIS OF PROCEEDINGS

Combating Health Care Fraud & Abuse: Technologies and Approaches for the 21st Century

June 26-28, 2000
Crystal City, Virginia

Conference Sponsors:

U.S. Department of Health and Human Services
Health Care Financing Administration
&
U.S. Department of Justice

Prepared by:

Howard Cohen
Health Care Financing Administration
Baltimore, Maryland

Steven G. Shandy
U.S. Department of Justice
Washington, D.C.

Susan Hahn Reizner
Health Care Financing Administration
Chicago, Illinois

Carol Cribbs
U.S. Department of Justice
Washington, D.C.

Combating Health Care Fraud & Abuse: Technologies and Approaches for the 21st Century

This document offers an overview of the proceedings of a national conference, cosponsored by the U.S. Department of Health and Human Services' Health Care Financing Administration (HCFA) and the U.S. Department of Justice (DOJ), which explored technologies and approaches to combat health care fraud and abuse in the 21st Century. The conference was held from June 26-28, 2000, in Crystal City, Virginia.

Keynote addresses by HCFA Deputy Administrator Michael Hash and Deputy Attorney General Eric Holder highlighted the program.[1] The conference drew nearly 300 attendees from a wide universe of health care program and law enforcement officials dedicated to combating fraud and abuse in Medicare, Medicaid, and other government health programs. Attendees included staff from HCFA Central and Regional Offices, Medicare contractors, Medicaid State Agencies, other Federal health programs, Medicaid Fraud Control Units, the Department of Justice, U.S. Attorney's offices, the Federal Bureau of Investigation, the Department of Health and Human Services' Office of Inspector General (OIG) and other Federal and state law enforcement agencies. Enriching the experience were exhibits by more than 25 vendors displaying the latest in electronic fraud and abuse detection technologies.

The conference focused on two basic themes. The first was an exploration of where technology is driving the science of fraud detection in the 21st Century. Tools incorporating advanced data mining, neural networking, fuzzy logic and artificial intelligence hold great promise for identifying program vulnerabilities earlier than ever. These tools can propel us toward our goal of paying the right amount to the right provider the first time, instead of paying and chasing. Speakers emphasized, however, that no matter how sophisticated the tools or the science behind them, the art of fraud detection involving good analytical and investigative personnel is key to achieving optimal results.

The conference's second theme addressed approaches to combating fraud and abuse. Advancing technology makes it all the more vital that all stakeholders involved in combating health care fraud and abuse maintain close partnerships. Because bad actors do not discriminate among health programs they defraud, joint program integrity efforts are increasingly important. And because law enforcement frequently lacks the technical expertise to fully appreciate sophisticated data analysis, close interaction is required between law enforcement and analytical/investigative staff. Although these demands sound simple, they raise complex legal and policy issues, including significant privacy implications and practical concerns about how to effect collaboration.

[1] Mr. Hash assumed the role of Acting Administrator of HCFA in October 2000.

Table of Contents

Executive Summary

The Federal government spends nearly $38 billion a year on operating systems, software, telecommunications, existing infrastructure, and data centers that affect agencies' abilities to safeguard government health insurance programs. Updating conference attendees on developments and future directions within the U.S. Department of Justice (DOJ), Deputy Attorney General Eric Holder discussed an evolving program integrity strategy. The sophisticated tools and ***science*** of fraud detection are most effectively unleashed when the proper balance is achieved with the human element: the analytical and investigative skills inherent in the ***art*** of fraud detection.

Mr. Holder credited close cooperation among law enforcement and Federal agency staffs who used sophisticated data analysis for a record-breaking $486 million settlement in a health care fraud case that began as a *qui tam* false claims suit. Data analysis, which was one of six methods used to verify allegations, focus the investigation, and prove fraudulent billing practices, enabled investigators to grasp the enormity of the case and direct their resources efficiently. Far from eliminating the need for traditional investigation, the technology-centered development of this case taught lessons about the characteristics of a successful data analysis team. It requires players with clinical expertise as well as policy and practice knowledge, and data analysis players who must communicate with each other.

Proactive at the outset - The DOJ will continue to maximize the collaborative use of both the art and science of fraud detection as it focuses on emerging priority areas, including nursing home and long-term care, a possible prescription drug benefit in Medicare, and the dynamic growth of the Internet to deliver health information, goods and services. Mr. Holder encouraged the Department of Health and Human Services (DHHS) to continue to collaborate with DOJ and other stakeholders to identify program vulnerabilities at the outset of any new benefit program, to heed lessons learned by State Medicaid Agencies already offering such benefits, and to consider the best ways to use technology.

Michael Hash, Acting Administrator of DHHS' Health Care Financing Administration (HCFA), reported that HCFA's success in employing high tech tools to combat fraud was instrumental in reducing the Medicare claims payment error rate from 14 percent in Fiscal Year (FY) 1996 to 7.97 percent in FY 1999, helping to extend the solvency of the Medicare Trust Fund. A critical program integrity issue for Medicare, however, is the need to achieve yet another critical balance: keeping bad providers out of the system without losing faith with the good players who account for the majority of providers and suppliers participating in the Medicare program.

Mr. Hash stressed the importance of coordination between agencies so that the benefits of curbing fraud via the use of technology – including the "tremendous horsepower of high performance computers" – can be shared. Touching on the interplay of art and science in fighting fraud, Mr. Hash also stressed that even in a technology-driven era, the human element remains "the lynchpin in a continuum" in which science enhances the art of collaboration and information sharing. "Federal and state health care programs, and federal and state law

enforcement, must join in collaboration . . . to ensure that we all benefit from our partners' unique data analysis methods and results," Mr. Hash said.

State activity - State Medicaid Agencies concurred that as crucial as their information technology (IT) investments are, traditional investigative methods such as onsite reviews and interviews remain as important as ever. IT initiatives, including data mining and newer surveillance and utilization review subsystems (SURS) that offer real time processing and substantially faster reports, have been implemented in many states. Some states have adopted sophisticated neural-based systems based on the "predictive model" that protects 85 percent of the nation's credit card businesses. Unlike a static fraud detection method that quickly can become ineffective, this dynamic model uses intelligent technology to continually evolve and "learn" to recognize unexpected and suspicious patterns of activity.

Although highly effective in detecting emerging scams, the resource intensive nature of neural technology poses its own challenges, however. It is expensive and demands heavyweight support from analytic staff ("the original neural net," in the words of one presenter) to maintain a working balance of art and science. Beyond the challenges of updating often-outdated fraud detection systems, State Medicaid Agencies also face the need to foster collaboration among themselves and with Federal health and law enforcement agencies.

Prepay vs. "pay and chase" - Denying claims on prepayment review yields from five to 15 times more savings than attempting to recover overpayments based on postpayment review. Data mining and neural networks are effective in detecting new scams so prepay controls can be implemented and investigations triggered. To be useful to law enforcement for case development and for presentation to a jury, however, it is critical that any early warning tool used be easily justified and explained.

Other promising tools - A review of new electronic fraud detection (EFD) information systems included discussion of a subset of EFD systems that incorporate clinical-based data in profiling providers. Using an epidemiological approach, these tools classify patients based on diagnostic codes and can calculate actual versus expected treatment costs. This type of system is a promising new weapon for fighting fraud because it can detect possible underutilization of services as well as overutilization.

Software packages - To maintain a competitive marketplace, HCFA has not adopted a standard EFD software package. Vendors also have been unable to develop Medicaid fraud detection software packages due to program variances from state to state. HCFA contracted for an evaluation of 10 EFD systems in real-world use. The report concluded that there is no single, comprehensive EFD system, and those who use EFD technologies tend to use a "suite" of systems. Regardless of the science used, the human factor in the art of fraud detection surfaced in the report, which concluded that even the best technology might go unused without buy-in from program integrity staff. Vendor support also is critical in determining a system's future customization, life cycle costs, and reliability of technical support.

Medical record privacy - The use of EFD tools intersects with a discussion of medical record privacy, which is a high priority for both DHHS and DOJ. The Supreme Court has observed that modern medical practice involves disclosures of medical information to third party payers, public health agencies and others, and concluded that patients no longer can reasonably expect their general medical records to remain completely confidential.[2] Notwithstanding this, the Department of Justice has issued a series of memorandums and guidelines, most recently on August 30, 2000, which underscore the Department's commitment to protecting medical record privacy consistent with case requirements, and which address a number of steps that Department employees should consider to protect the privacy of any health information obtained by the Department for investigations and case matters.[3] Any EFD database matching projects involving federal systems of records should be reviewed for compliance with the computer matching requirements of the Privacy Act (5 USC 552a(0)) and with the requirements of the Substance Abuse privacy regulations (42 CFR Part 2).

The new Department of Health and Human Services "Standards for Privacy of Individually Identifiable Health Information, "45 CFR Part 164, published on December 28, 2000, will generally continue to allow broad disclosure of health care information to health oversight agencies for such purposes as fraud and abuse detection and prosecution, though these disclosures will be subject to a requirement that only the "minimum necessary" information may be disclosed. Covered entities will be permitted to rely on the representation of a health oversight agency that the requested disclosure is the minimum necessary. These rules will not be effective, however, for any "covered entity" until February 26, 2003, while covered entities defined as "small health plans" will have until February 26, 2004 to comply with the new requirements. A correction published in the federal Register on December 29, 2000 makes clear that until these effective dates, the privacy standards cannot be cited by covered entities to resist requested disclosures.

Task force model - Messrs. Holder and Hash suggested in their opening comments a goal that reverberated throughout the rest of the conference: forging alliances and networks that would thrive well beyond the end of the conference. Detailing "next steps" that can be taken to develop data into successful investigations, a Special Agent of the Federal Bureau of Investigation (FBI) described a federal/state health care task force that collaborates on fraud schemes, information

---

[2] For example, enrollees in government health care plans such as Medicare, Medicaid, or the Federal Employees Health Benefit Program routinely sign consents for disclosure of health information in order to document and verify claims for third-party payment submitted to those health care plans. Furthermore, providers who submit claims to health plans on behalf of patients routinely certify that they have a consent form from the patient on file which authorizes such disclosures.

[3] Presidential Executive Order 13181, dated December 20, 2000, mandates a new review by the Deputy Attorney General (or the General Counsel of the Department of Defense for military medical records) when medical records disclosed during health oversight activities reveal evidence of non-health-care crimes, each time federal investigators or prosecutors would like to use the evidence in those records to pursue the non-health-care matter.

needs and ongoing investigations. Participation in task forces helps alleviate an inherent tension between the immediate interests of program agencies to "stop the bleeding" by recovering losses, and the longer-term interests of law enforcement agencies to develop cases. The director of a State Medicaid Fraud Control Unit recommended that program agencies bring prosecutors into fraud investigations early, and that everyone keep the lines of communication open.

Describing another example of the many task forces in which program agencies and law enforcement are sharing information, a Medicare contractor has developed a payment safeguard steering committee comprised of Parts A and B and durable medical equipment staff, who coordinate and alert each other to pending investigations. The contractor maintains a computerized bulletin board to further enhance information sharing.

Data sharing - One FBI field office also has developed a routine process and standardized format for obtaining data extracts from Medicare and Medicaid program agencies and contractors service the office's geographic area. The administrative simplification standards of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law No. 104-191) will facilitate data standardization and break down barriers to sharing information for law enforcement purposes.

Workgroup recommendations - Interactive, regionally based workgroup sessions gave participants the opportunity to discuss issues raised during the plenary and breakout sessions. The workgroups offered recommendations for specific follow-up action, which HCFA and DOJ have developed into an Action Plan for the future. Many regional workgroups recommended the formation of a National Technology Group to address crosscutting issues raised during the conference, to serve as an information clearinghouse, and to facilitate formation and coordination of Regional Technology Users' Groups. The workgroups also noted that existing multi-agency, multi-level task forces, need to be reinforced. They asked that HCFA continue to expand its fraud and abuse initiatives, citing educational activities in particular. Finally, workgroup participants agreed on the need for future conferences at which federal and state regulators and contractors can share the issues, ideas and strategies that inform their use of technology to combat health care fraud and abuse.

Keynote Presentations:
Eric Holder, Deputy Attorney General, U.S. Department of Justice
Michael Hash, Deputy Administrator, Health Care Financing Administration

Eric Holder, Deputy Attorney General, U.S. Department of Justice
U.S. Department of Justice Deputy Attorney General Eric Holder, Jr. presented the first keynote address.[4] Mr. Holder noted the commitment that Attorney General Reno has made since the beginning of her tenure to combat health care fraud, and how that commitment has been realized. Since 1993, the number of attorneys devoted to health care fraud has increased five-fold and the number of FBI agents investigating health care fraud has tripled. From Fiscal Year (FY) 1993 to the present, the annual number of criminal health care fraud convictions and civil health care fraud investigations has quadrupled, and civil health care fraud case filings have tripled.

The enactment of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law No. 104-191) helped cement the partnership among the Department of Justice (DOJ), the Department of Health and Human Services' Office of Inspector General (DHHS OIG), and the Health Care Financing Administration (HCFA). Initiatives launched by these partners have resulted in the recovery through restitution and criminal and civil fines of nearly $2.5 billion, much of which has been restored to the Medicare Trust Funds.

Mr. Holder spoke about a recently resolved case that yielded the largest health care settlement to date. In a case that originated as a "whistle blower" suit under the False Claims Act, National Medical Care (NMC), the largest dialysis services provider in the United States, was alleged to have submitted false claims for nutritional supplements, clinical laboratory tests, and diagnostic tests; to have conspired to pay illegal kickbacks; and to have failed to report and repay credit balances and other overpayments received from Medicare. Sophisticated data analysis, facilitated by close cooperation between law enforcement and multiple Federal health oversight agencies, helped prove that NMC had engaged in a wide-ranging conspiracy to defraud Medicare and other Federal health insurance programs. NMC agreed to settle the case in January 2000 by paying the Federal government $486 million in criminal fines and civil restitution and penalties.

The DOJ is focusing particularly on several immediate and emerging priorities where effective use of technology and interagency partnerships will be keys for ensuring appropriate health care fraud prevention and enforcement, Mr. Holder said. These priority areas include: (1) nursing home and long-term residential care; (2) possible expansion of Medicare to include a prescription drug benefit; and (3) the exploding growth of the Internet to provide health information and sell health care goods and services.

First, many nursing homes have been found delivering seriously inadequate care, with residents, many frail to begin with, needlessly suffering from preventable pressure sores, malnutrition, and

[4] The full text of this speech may be found on the DOJ's Internet website at the following address: www.usdoj.gov/dag/speech.html

accidents. Recent efforts by HCFA and the DOJ offer grounds for optimism that such patient harm can be prevented, however. HCFA now uses "Minimum Data Set" quality indicators to better monitor residents" quality of care. Joint DHHS and DOJ conferences have led to development of an infrastructure and an action plan to protect vulnerable nursing home residents.

Second, as Congress and the Administration weigh alternatives to adding a prescription drug benefit to the Medicare program, the DOJ also is anticipating potential program integrity issues that could arise from such a benefit. Mr. Holder encouraged the DOJ and DHHS to work together to identify program vulnerabilities, to identify successful measures employed by State Medicaid Agencies that already offer such benefits, and to consider how technology may be applied to combat potential fraud and abuse from the outset of any such program.

Third, in light of the continuing increase in the use of the Internet in the health care arena, from dispensing drugs and medical devices to advice, Mr. Holder challenged law enforcement and government health agencies to take steps to identify vulnerabilities and to boost program safeguards without stifling the growth of this vital medium.

In closing, Mr. Holder also challenged attendees to be more than passive observers during the conference. He encouraged audience members to talk about their experiences with using "high-tech" tools to combat health care fraud and abuse; to exchange lessons learned, both from successes and from setbacks; to discuss challenges overcome and challenges that still lie ahead; and to help blaze a path to the future.

Michael Hash, Deputy Director, Health Care Financing Administration
Mr. Hash reviewed just how far the Medicare and Medicaid programs have come since their inception. The number of Medicare and Medicaid beneficiaries has risen from less than 30 million at the programs' outset to nearly 80 million today. Financing health care for one in four Americans, HCFA is the largest insurer in the world, overseeing annual health care expenditures of more than $300 billion.

While the several hundred million claims presented annually for payment in the early days of Medicare were nearly exclusively paper-based, said Mr. Hash, the nearly one billion claims now processed annually are presented almost exclusively in electronic form. HCFA's goal is to "pay it right" – paying the right amount to the right provider for the right service on behalf of the right beneficiary. To achieve this goal in this electronic environment, HCFA has become one of the nation's leading users of data and data analysis systems.

HCFA has enjoyed success employing high technology tools to combat fraud and to ensure that claims are paid right. Mr. Hash noted that the claims payment error rate as reported in HCFA's *Chief Financial Officer's Audit Report* dropped from 14 percent in Fiscal Year (FY) 1996 to 7.97 percent in FY 1999, and that the Agency has committed to further reducing the error rate to less than 5 percent by FY 2002. Tangible results like these have helped extend the solvency of the Medicare Trust Funds to 2025.

Mr. Hash expressed the importance of the conference in the continuing effort to meet HCFA□s program integrity goals, noting that "the tremendous horsepower of high performance computers will enable HCFA to analyze vast amounts of data to uncover trends and patterns we never knew existed, quickly enough to take meaningful action."

But, Mr. Hash emphasized that, even in this technology-driven era, the human element is the lynchpin in a continuum in which technology merely accelerates the process of sharing information among partners. Federal and state health care programs, and Federal and state law enforcement must collaborate to combat fraud schemes that are rarely confined to just one health program or one geographic area.

HCFA's program integrity goals differ somewhat with respect to Medicaid, as compared with Medicare, because States bear primary responsibility for detecting, prosecuting, and preventing Medicaid fraud, waste, and abuse. In Medicaid, HCFA functions as a partner with the states, providing funding and technical support in addition to oversight and education. HCFA has been working with the states, said Mr. Hash, to help them modernize and upgrade their Medicaid data management and information systems.

In closing, Mr. Hash joined Mr. Holder in encouraging attendees to network and forge alliances with colleagues during the course of the conference, and to strive to keep these interactions alive long after the conclusion of the conference.

Current Environment: Up and Running: *An overview of the Medicare Integrity Program, the National Medicaid Fraud and Abuse Initiative, and new initiatives within State Medicaid Agencies.*

Speakers:

Rose Crum-Johnson, Southern Consortium Administrator, HCFA
Penny Thompson, Director, Program Integrity Group, HCFA
Linda Wertz, Director, Texas Health and Human Services Commission and President, National Association of State Medicaid Directors (NASMD)

Medicaid Issues

- Some States have conducted claims payment accuracy rate measurement studies, which yield percentage figures estimating the total amount of overpayments in the States' Medicaid programs. Error rates include not just outright fraud, but also components of waste, abuse, and even innocent billing errors.

- Information technology (IT) initiatives are in place in a number of states, with Florida, Kentucky, North Carolina, Texas, and Washington having adopted neural based systems. Texas' Health and Human Services Commission has reported that $2 million in savings in the State's Medicaid program are attributable to the new system. As important as IT investments are, however, traditional investigative methods, including onsite reviews and provider interviews, should not be neglected.

- Forty-seven states maintain certified Medicaid Fraud Control Units (MFCUs), which operate separately from the State Medicaid Agencies and most often function under the auspices of the State Attorney General's office.

- A Federal regulation referred to as the "60-day rule" and found at 433 CFR 316 requires states to repay the Federal share of an overpayment within 60 calendar days of discovery, regardless of whether the State actually is able to recoup the money from the provider within that timeframe. States argue that this places a substantial and unfair burden on them.

- Led by HCFA's Southern Consortium, the National Medicaid Fraud and Abuse Initiative (Initiative) recently celebrated its Third Anniversary. Under the Initiative's precedent-setting organizational structure, a Medicaid Fraud and Abuse Team, based at HCFA's Central Office in Baltimore, reports to the National Coordinator of the Initiative in the Southern Consortium. The Initiative also includes a network of Medicaid Fraud and Abuse Coordinators who are based in all 10 of HCFA's regional offices across the country. Its unique structure positions the Initiative to be responsive to the States, and ultimately to be more effective in providing technical assistance, guidance and oversight to increase the effectiveness of the States' program integrity efforts.

- A Medicaid Fraud and Abuse Technical Advisory Group (TAG), formed in response to a need for better communication across state lines, serves as a forum to:

- share issues, solutions, and resources;
- develop best practices; and
- advise HCFA on policies, procedures, and practices to better coordinate efforts to combat fraud and abuse.

- Nineteen states currently are represented on the TAG, which has established a networking mechanism to ensure that all states are kept informed of its activities. The TAG is guided by five workgroups, which address the following issues: (1) legal and regulatory; (2) database; (3) pharmacy; (4) data sharing; and (5) OIG issues.

- The Initiative is developing *Guidelines for Addressing Fraud and Abuse in Medicaid Managed Care* to assist the full range of involved entities with strategies to better prevent, identify, investigate, report, and prosecute Medicaid managed care fraud.[5] In addition to these guidelines, the Initiative is developing a model compliance plan for Medicaid managed care organizations.

- HCFA's Fraud Investigations Database (FID) is being modified to include Medicaid cases.

- A survey of fraud detection systems employed by State Medicaid Agencies is underway, and will lead to publication of an IT *Systems Resource Guide*. Focusing on six systems-related areas, the survey is designed to gather information about the States' existing SURS and system enhancements; current features and capabilities of the states' systems; vendor products and services; the states' "wish lists" for future replacements and enhancements; and best practices for innovative data collection and reporting.[6]

- The Initiative maintains a comprehensive website listing of the official statutory citations of state legislation that is used to prosecute civil or criminal fraud, to maintain program integrity, and to combat program abuse (http://www.hcfa.gov/medicaid/fraud/mfs).[7]

- A national review team composed of HCFA staff on the Initiative's network of regional Medicaid fraud and abuse coordinators conducted onsite program integrity reviews of eight State Medicaid Agencies during FY 2000 to determine if the states are complying with applicable Federal laws and regulations. The review team also observed how the states'

---

[5] These guidelines became available in August 2000 and are available on the HCFA website at: www.hcfa.gov/medicaid/fraudgd.pdf.

[6] Completed information systems questionnaires subsequently have been returned to the Initiative's Information Systems Workgroup by 47 State Medicaid Agencies, reflecting a 93 percent response rate. The workgroup is in the process of compiling the *Systems Resource Guide* based on the survey data.

[7] The Initiative also has enhanced its general information site on the HCFA website at: www.hcfa.gov/medicaid/fraud.

Medicaid program integrity staffs handle information regarding potential fraud and abuse, and how they relate to other entities. The results of these reviews will be summarized in a report that will be completed in FY 2001. Reviews of Medicaid program integrity efforts in another eight states have been scheduled by the Initiative for FY 2001.

- In 1999, HCFA contracted with Dr. Malcolm Sparrow to facilitate a series of executive seminars on Medicaid fraud control coordinated by the Initiative. The seminars aimed to strengthen state efforts and to encourage coordinated fraud and abuse control efforts. Key observations from these seminars included:

  - The need to build commitment, understanding, support and resources for fraud and abuse control efforts;
  - The need to access claims databases, claims analysis, and fraud and abuse detection technology (a number of states reported that innovations were being implemented, while others reported antiquated technological infrastructures); and
  - The implications of fighting fraud and abuse in a managed care environment.

- Significant challenges lie ahead, including identifying new products to upgrade outdated fraud detection systems, encouraging State Medicaid Agencies to continue to work together, and fostering collaboration between Federal and state health programs.

Medicare

- A critical program integrity (PI) issue is the need to strike a balance in fraud deterrence, detection, and enforcement efforts to keep the few "bad guys"out of the program without losing the confidence of the "good guys" who constitute the vast majority of Medicare providers and suppliers.

- Medicare PI efforts have become proactive and forward thinking, with workgroups, for example, already assessing potential vulnerabilities that may lie in a Medicare outpatient prescription drug benefit.

- HCFA in early 1999 issued a *Comprehensive Plan for Program Integrity* that is comprised of two major components:
  1. Improving HCFA program integrity management; and
  2. Addressing service-specific vulnerabilities.

- Within the Medicare PI management component are five elements, many of which have been already achieved:
  1. Increasing the effectiveness of medical review and benefit integrity activities;
  2. Implementing the Medicare Integrity Program;
  3. Implementing payment safeguards under provisions of the Balance Budget Act of 1997 (BBA) Public Law No. 105-33);

4. Promoting provider integrity; and
5. Year 2000 (Y2K) contingency planning.

- Established as part of HIPAA, the Medicare Integrity Program (MIP) brought a stable source of funding to HCFA's PI efforts. Increased resources and authority concomitantly increase HCFA's accountability. MIP-funded program integrity activities include medical review, fraud detection, and cost report auditing. Under its MIP authority, HCFA conducted a competition through which a schedule of 13 Program Safeguard Contractors (PSCs) was established. Each PSC is qualified to conduct a full range of PI activities, including medical review, fraud investigation, cost report auditing and provider education. The 13 PSCs competitively bid among themselves on MIP task orders.

- Initially, five task orders were issued, addressing:
  - An assessment of Y2K vulnerabilities;
  - Corporate integrity agreement compliance review;
  - Provider education effort addressing "good provider" error avoidance;
  - Cost report auditing; and
  - A Benefit Integrity Support Center (BISC), which is a geographically based center for data analysis focused on identifying fraud schemes.

- Four PSCs under development include:
  1. A Statistical Analysis Center where data mining techniques will target geographic areas;
  2. The Western Integrity Center, which will conduct data analysis, fraud detection, and postpay analysis for a number of western states;
  3. Therapy Analysis Support Center, to determine error rates for therapies administered in home health settings and skilled nursing facilities, following provisions of the Balanced Budged Refinement Act (BBRA) that lifted earlier-imposed therapy payment caps; and
  4. Comprehensive Error Rate Testing, to establish baseline payment error rates for each HCFA claims processing contractor.

- In response to audience questions, panelists stated that:
  - HCFA is exploring proposed methodologies on how to calculate what percentage of its payments may be fraudulent, but ultimately it may not prove possible to develop a reliable measure to "know the unknowable."
  - Beneficiary interviews to detect fraud are sometimes appropriate, but they have their limits. Because an individual's recall is frequently poor, the services must have been rendered recently for this kind of interview to be effective. Moreover, due to the complexity of some medical services and the fact that some of them, such as laboratory services, take place remote from a patient, a beneficiary may not have a clear understanding of the services at issue in the interview.

Tools for the Times: *A review of the new electronic fraud detection (EFD) information systems designed to detect fraud and abuse through statistical analysis with an emphasis on how they differ in methodology and output. Topics included the workings of statistically driven case findings, the differences between population-based and provider-based analysis, rule driven versus relational standards for detecting aberrant patterns, and systems that can be used in the fee-for-service and capitated environments.*

Speakers:
Jean Bishop, PriceWaterhouse Coopers (moderator)
Karen Kaldal, VIPS Healthcare Information Solutions
Manon Ruben, Codman Group
Charles Schott, International Business Machines
Nick Skovran, Veritus Medicare Services

Note: This session featured demonstrations of several commercially available fraud, waste, and abuse detection products. A number of similar products are available in the marketplace, and HCFA offers no endorsement of any fraud detection product.

- Common fraud, waste, and abuse detection techniques include:
  - Searching for statistical outliers, *i.e.,* rankings or scores;
  - Rules violators;
  - Pattern recognition;
  - Random or periodic audits; and
  - "Widening the net," examining practitioners who fall at the "tip of the iceberg."

- General goals conveyed by clients include the desire to:
  - Save time and increase the efficiency of the fraud unit;
  - Conduct proactive fraud, waste, and abuse detection;
  - Reduce paper burden; and
  - Make analysts more autonomous.

- Key to all systems is the claims data, including such elements as: date(s) of service; procedure / revenue codes; identity of the provider; identity of the patient. Many, if not most, systems are packaged with ad hoc search capacity as well as a number of standard analytical reports. Effective systems should facilitate use of analytic tools to determine whether an initial trend or finding may indicate a possibility of fraud or abuse. Some systems also help manage and track research undertaken to develop potential cases.

- A subset of detection systems brings clinical-based data into the profiling of providers. Using an epidemiological approach, these products classify patients based on diagnostic codes, and can calculate actual versus expected billing and cost for treatment. By looking at the variance between the expected and actual billing and cost, these systems can single out specific claims and patients responsible for making a provider an outlier. By organizing care events into episodes, these systems can compare provider performance for similar episodes of

care. Geographic analyses are possible by which analyses of providers and beneficiaries can be linked to a geographic area.

- Epidemiological based systems may prove especially valuable in the evolving arena of managed care, as the analytical approach can help detect underutilization as well as overutilization.

Medical Records Privacy: *A focused discussion on medical records privacy and electronic fraud detection tools.*

Speaker:

Ian DeWaal, Senior Counsel, Criminal Division, Fraud Section, US Department of Justice

---

- Maintaining medical record privacy to the greatest extent possible is of great importance to the law enforcement community generally, including DOJ, as the public must be assured of the integrity of the criminal justice system and entrust that the "system" will be sensitive to doctor-patient confidences.

- HCFA carriers, fiscal intermediaries (FIs), and program safeguard contractors (PSCs) share a common interest in ensuring program integrity by eliminating fraud and abuse, and will have significant interaction with law enforcement. This interaction will occur when law enforcement requests data:
  - Pertaining to criminal investigations or *qui tam* ("whistleblower") cases;
  - Reviews to identify aberrant billing and payment patterns;
  - Pursuant to the program safeguard contractor statement of work; or
  - Pursuant to the HCFA-DOJ memorandum of understanding.

- The Attorney General has elevated medical records privacy issues to a high priority within DOJ. Procedures are found in the *Guidelines for Implementing the HIPAA Fraud and Abuse Control Program--Subsection VI--Confidentiality Procedures: Use of Information and Data (1/97).* The Deputy Attorney General also issued a memorandum, which applies to all DOJ cases and not just health fraud cases, entitled, *Protection and Confidentiality of Individually Identifiable Medical Information,* dated October 15, 1998. Further guidance was effective on August 30, 2000, from the Deputy Attorney General, entitled, "Suggested Practices for Maintaining the Confidentiality of Medical Records."

- Confidentiality issues inevitably will arise in the context of civil and criminal health care investigations and prosecutions. Law enforcement takes into consideration a number of issues when the need arises for individually identifiable information. Strategies that law enforcement may take may include:
  - Tailoring requests to avoid confidentiality issues;
  - De-identification;
  - Compartmentalization, requesting only those portions of the medical record likely to contain evidence of the alleged fraud.

- Confidentiality issues vary depending on the type of medical record. Types of medical records include general medical records, psychiatric treatment medical records, substance abuse patient medical records, medical records of patients with "socially stigmatizing diseases," and peer review organization medical records.

- In general, Federal supremacy laws supersede any state confidentiality protections. In processing and analyzing claims, contractors are considered HCFA's agents, and the records they process are considered official HCFA records.

- With regard to "general" medical records, the U.S. Supreme Court has held that because modern medical practice brings with it a number of disclosures essential to such practice, including disclosures to third party payers, public health agencies, and other medical personnel, individuals no longer should reasonably expect medical records to remain completely confidential. Some courts have held that there is a qualified privilege for medical records sought by search warrant or subpoena, which must be balanced against the interests of those attempting to obtain disclosure. One court set forth the factors to consider in this balancing test, which include:
  - Type of record requested;
  - Type of information it does, or might, contain;
  - Potential for harm in any subsequent nonconsensual disclosure;
  - Injury from disclosure to the relationship in which the record was generated;
  - Adequacy of safeguards to prevent unauthorized disclosure;
  - Degree of need for access; and
  - Whether there is express statutory mandate, articulated public opinion, or other recognizable public interest militating towards access.

- Administrative Investigative Demands for health care fraud investigations (Title 18, U.S.C. §3486) demonstrate a Congressional intent to override patient privacy to permit disclosure to the DOJ and FBI for criminal fraud investigations (but contain a limitation on derivative use of records against the patient, which were disclosed for the purposes enumerated in the provision).

- Psychiatric medical records warrant special treatment, as highlighted in a U.S. Supreme Court case, Jaffee v. Redmond, where the Court recognized a psychotherapist privilege for psychotherapy counseling notes. The privilege is not absolute, and exceptions are still evolving. Instances in which it may be overcome include:
  - Where there is a "serious threat of harm to the patient or to others which can only be averted by means of disclosure";
  - When waived by the patient;
  - Potentially, where payment for the care rendered is made by a third-party payer as opposed to directly from the patient; or
  - Potentially, when the provider is under investigation.

- Distinctions can be drawn between "confidential communications" made during the course of therapy, and other documents and records not containing these confidential communications, obtaining disclosure of which would generally be less difficult.

- Special disclosure rules also pertain to substance abuse medical records. The statutory

and regulatory frameworks are set forth in 42 U.S.C. §290dd-2(a) and 42 CFR Part 2. In general, these provide strong confidentiality protections and permit just narrow exceptions for disclosure of any substance abuse medical records generated by substance abuse programs that are "federally assisted." In general, disclosure of such records can be made only pursuant to written patient consent, pursuant to court order, or, within certain boundaries, for audit or evaluation purposes. Those making unauthorized disclosures are subject to fines, but there is no private right of action.

- Peer Review Organization (PRO) records are generally protected from disclosure by statute (42 U.S.C. §1320c-9(a)). Patient records in the possession of a PRO operating under a contract with the Secretary of DHHS are not subject to subpoena in civil proceedings per 42 U.S.C §1320c-9(d)). An exception permits PROs to disclose information that identifies specific providers or practitioners to Federal and state agencies recognized by the Secretary as having responsibility for identifying and investigating cases or patterns of fraud or abuse at the request of such agency as relates to a specific case or pattern.

- Providers submitting third-party reimbursement claims to government or private health insurance programs will have in a patient's file Assignment of Benefits forms authorizing third-party billing as well as the release of medical information and records to verify the claim. Similarly, HCFA's forms submitted by providers for third-party reimbursement contain certifications made by the provider that the provider has on file a release from the patient permitting third party billing and an authorization from the patient to disclose medical records to verify billing.

- Health and other information held by the Federal government is governed by the Privacy Act, 5 U.S.C. 552a. Computer matching agreements are required when a Federal agency desires to use another agency's data (defined at the Departmental level) or state or local government data to verify continuing eligibility for federal government benefits. Certain exceptions apply to agencies whose primary functions are criminal law enforcement. Some "systems of records" held by some Federal agencies have "routine uses" that permit disclosing evidence of criminal activity to a law enforcement agency. There is a memorandum of agreement in place between HCFA and the DOJ with respect to data sharing that facilitates the DOJ's access to HCFA data required for a use consistent with a published "routine use" (a term of art under the Privacy Act) in the system of records notice for that data. Law enforcement agencies also may request protected information under the law enforcement exception at 5 U.S.C. 552a(b)(7).

- The Department of Health and Human Services published the Final Rule on "Standards for Privacy of Individually Identifiable Health Information," at 63 Fed. Reg. 82462, on December 28, 2000. Technical corrections were published on December 29, 2000, at 63 Fed. Reg. 82944. The rule is scheduled to take effect on February 26, 2003, except for "small health plans," which will have until February 26, 2004.

Data Analysis, Next Steps, and Obstacles to Effective Collaboration: *What types and levels of problem providers and billing patterns are identifiable and what "next steps" may be taken to confirm and develop data and reports into fruitful investigations, prosecutions, and/or financial recoveries? What obstacles hinder effective use of fraud detection technology for these purposes and how can new tools, statistical sampling, and other approaches help overcome traditional obstacles?*

Speakers:
Linda Wertz, Director, Texas HHS Commission, and President NASMD (moderator)
G. Clayton Grigg, Special Agent, Federal Bureau of Investigation, El Paso
John Krayniak, Director, Medicaid Fraud Control Unit, State of New Jersey
Noel N. McKetty, First Coast Services Options
Paul A. Rustigian, Auditor, District of Massachusetts**,** US Department of Justice

---

- This session featured speakers discussing the impact of data analysis systems in the evolution of health care fraud cases from detection to investigation and statistical sampling, and, ultimately, civil action or criminal prosecution.

- A representative from a Medicare contractor discussed a trend analysis of claims data for Comprehensive Outpatient Rehabilitation Facilities (CORFs). Trend analysis revealed that monthly payments to CORFs in a certain geographic area rose from $4 million per month to $6.5 million per month and corresponded to a change in the coverage limits for physical and occupational therapy.

- Two facilities were found to account for two-thirds of the overall increase in payments to CORFs. Surveys of beneficiaries treated at the two CORFs revealed that the services billed for one of the two providers were legitimate while those billed for the second provider were not. A case referral was prepared for the second provider, was presented and accepted for investigation by the FBI, and was successfully prosecuted by DOJ.

- Several data analysis approaches are used by the FBI's El Paso field office to examine health care claims data for possible evidence of fraud in response to specific allegations of fraud for ongoing investigations. This field office has used data analysis methods to successfully develop and investigate health care fraud for cases involving physicians, home health, clinics, rehabilitation facilities, and durable medical equipment suppliers, and has developed data analysis models that could be used for cases involving pharmacies and mental health facilities.

- This field office has developed a routine process and a standardized data format for obtaining extracts of Medicare and Medicaid data for beneficiaries located within the office's geographic area. Representatives of the FBI and other Federal investigative agencies, state and Federal health insurance programs, the Texas MFCU, and U.S. Attorney's office participate in a Federal/State health care fraud task force that meets on a quarterly basis to

share information about fraud schemes, address information needs and problems, and to coordinate ongoing investigations. The task force also uses "break-out groups" to focus its work on specific investigations.

- Health care fraud cases may be developed through statistical sampling and claims analysis. The statistical sampling approach of the Boston U.S. Attorney's Office (USAO) in the National Medical Care case served as an illustration. A speaker from the USAO offered the following suggestions for others who may use statistical sampling in future health care fraud cases. Where possible:
  - Design and plan the sample to be admissible in court in case the sample must be defended in litigation; consult with a statistician during all phases of the sample (i.e., planning, designing, implementing, and evaluating).
  - Sampling should be a slow process that should not be rushed. Sampling should not be conducted in a "vacuum."
  - Analyze claims data and the claims universe prior to planning and designing the sample; you should know before you design and implement the sample the nature, scope, and characteristics of all items potentially in the universe.
  - Be conservative when designing the sample; study the population and reduce variability when possible. Define the universe carefully, considering service types and dates and matching to cost report periods, if appropriate.
  - Share the sample planning, design, implementation, and results to date with the defendant up front, when appropriate and after consultation with prosecuting attorneys.
  - Choose well-credentialed experts on whom you can rely to inform you of the strengths and weaknesses of your case theories.

- Prosecutors must take information suggested by data analysis and fraud detection tools and acquire other evidence to prove the falsity of claim and culpability of individuals making the false claims. For example, prosecutors must be able to prove who was the source of the data represented on a claim, the "chain of custody" for claims information, the accuracy of data analysis and fraud detection programs, and obtain corroborating evidence through search warrants, grand jury testimony, wiretaps, and other investigative methods to prove that intentional fraud occurred.

- Frequently there is tension between Federal and/or state program agencies and criminal prosecutors because program agencies want to "stop the bleeding" by recovering losses through civil and administrative remedies while criminal prosecutors typically want to develop cases for possible criminal convictions and program exclusions. As a result, health care programs and investigative agencies should bring prosecutors into fraud investigations early, through consultations or task forces, so they can discuss and screen potential cases to determine the most appropriate course of action based on the type of evidence of possible fraudulent intent, and the future impact on the program associated with the type(s) of sanction(s) that may be imposed.

Evaluating Systems: *An in-depth discussion of issues to consider when evaluating systems. Topics addressed included: How can systems best be compared/evaluated when there are no established benchmarks? How can multiple systems (a "suite of systems") be incorporated in one operation to achieve best results? How can one ensure the system fits the scope of the operation? Is it best to install a system or opt for a service bureau approach? What skills are needed in an analytic staff to take advantage of new technologies?*

Speakers:

George Mills, Director, Division of Methods & Strategies, Program Integrity Group, HCFA
Thaine Allison, T. H. Allison & Associates
Dennis Cowan, Arthur Andersen Consulting
Rick Friedman, Director, Division of State Systems, Center for Medicaid and State Operations, HCFA
Eric Martin, McNeil Technologies, Inc

- To maintain a competitive marketplace that encourages innovation, HCFA has not adopted standard electronic fraud and abuse detection software. Even if there were some intent to adopt a standard package, however, it would be extraordinarily difficult to evaluate and compare systems because there are no benchmarks.

- Under a contract with HCFA, a catalog evaluating 10 fraud, waste, and abuse software detection systems was prepared in 1999. Several site visits were made to HCFA contractors to see the applications in real-world use, and the product vendors offered demonstrations of features. Evaluation criteria included product cost, operating platforms, and the strengths and weaknesses of the applications' features as they pertain to Medicare program integrity efforts.

- The report concluded that there is no "perfect" electronic fraud and abuse detection system. Those who use such tools tend to employ a "suite" of analytical systems. For example, a claims processing and benefit integrity (BI) contractor might accomplish a number of BI functions using features integral to the claims processing system, supplemented as necessary with specialized BI applications. A typical suite may include an analytical system, a case management and tracking system, a claims processing system, and various reference databases. Regardless of the electronic tool, personnel are the real keys to success.

- According to the report, application selection criteria should include: (1) assessment of the specific analytical need; (2) implementation / integration issues; (3) product delivery format; (4) life cycle costs; and (5) availability of technical support. Determine all departments/components within an organization that may have a need to use the application, and assess their needs. Often it is useful to denominate a champion from within the organization who has knowledge of the goals, and ability to build a consensus and support from prospective users. Without "buy-in" even the best technology may go unused.

- An initial part of the cataloging effort consisted of developing a comprehensive list of application functionality with which to gauge the products cataloged. An organization considering acquiring a tool cannot spend too much time examining its specific analytical requirements, looking at the tasks it undertakes, considering whether it may perform different or new tasks in the future, and concisely specifying these requirements.

- Implementation burdens should be accounted for, with the burden frequently varying with the degree to which the application has been customized for its intended use. Be alert as to the server type(s) and/or platform(s) with which the system is compatible. Technical and analytical support personnel are critical, and new systems may present new staffing requirements. New models and report templates likely will need to be generated for the new system. One to two month implementation times are not infrequent.

- Applications may be offered in several formats, including: (1) turnkey models; or (2) service bureau models. There are numerous factors to consider with either route. Service bureau models offer minimal commitment at limited cost, and with offsite programming and data analysis, few training issues. Downsides, however, may include the inability to rapidly run new or modified queries, as well as security and confidentiality issues from having to transmit data off-site may generate security and confidentiality issues. Turnkey solutions may present high installation costs, issues of compatibility with present systems, and requirements for additional staffing, but may offer the investigative staff tremendous flexibility.

- In any case, vendor support is critical. Issues to consider are whether the system can be customized as needs change, what the life cycle costs will look like, and the accessibility and reliability of technical support.

- Application costs will extend past an initial purchase. Be aware that low bids are not necessarily the best determinative criteria. Life cycle costs may include:
  - System costs beyond software;
  - Hardware/software upgrades;
  - Varying size of operation (charges on numbers of claims processed or the dollar value of those claims, number of years of data processed, etc.);
  - Maintenance fees;
  - Licensing fees for the application and/or for products incorporated into the application; and
  - Requirements for additional staffing, including technical support and programmers.

- Exercise due diligence before making any system acquisition. Available technical support should be closely scrutinized. Speak with other users, visit their sites, and ask how long it took to achieve a return on their investment. Look for well-structured support systems that include help-desks, and assess the ease or difficulty of having questions addressed.

Scrutinize the vendor's history of regularly updating the product. Require vendors to provide demonstrations, even demonstrating analytical capabilities on live data. Clearly convey to vendors the organizations requirements, including where the system will be placed, whether it will be applied in pre- or postpay uses, and whether it will be a primary or secondary system.

- The Federal government will pay 90 percent, with the state assuming the other 10 percent, of the cost to design, develop, and test a new Medicaid Management Information System (MMIS). Once operational, the Federal government will pay 75 percent of the continuing operating costs, with the state paying the remaining 25 percent. The Federal government will not pay for the development or acquisition of proprietary fraud and abuse detection products, but will pay for continuing operating costs. The Federal government will contribute varying amounts for other fraud and abuse detection solutions incorporated outside of the MMIS. (*see* 433 CFR 110 *et seq*.)

- Medicaid fraud and abuse staffs tend to be disproportionately small as compared with their Medicare counterparts.

- Vendors are frustrated in their efforts to develop Medicaid fraud detection software packages because each state Medicaid program is so different. These variations also present more opportunities for providers to become confused, while enabling others to take advantage of the situation to actively defraud the programs. IT solutions should play a large part in provider education, while remaining vigilant to looking for corrupt providers.

- A system should be able to:
  - Help establish baselines;
  - Help analyze the impact of policy decisions to assess effectiveness;
  - Interface with a data warehouse; and
  - Enhance the SURS subsystem, (i.e., SURS can retrieve current data that then can be manipulated with PC software to analyze aberrant patterns).

- HIPAA's Administrative Simplification provisions will standardize some data across boundaries (*i.e.*, patient identification number, provider identification number, etc.), breaking down some of the present barriers that exist at State lines. The potential downside to this, however, is that any errors may be exacerbated as they ripple through the system.

- Although the ever-increasing number of dually eligible beneficiaries increases the need to communicate between the Medicare and Medicaid programs, organizational culture and technological issues hinder communication.

- States must establish their own policies for use of the Internet for data collection, in which they will have to weigh the flexibility and benefits the Internet may offer with the omnipresent privacy and security concerns.

Case Finding by the Numbers: Statistical Methods of Fraud Detection and Case Development: *Electronic Fraud Detection (EFD) greatly expands the case finding capacity of Federal and state health programs -- Then what? Will EFD become the primary source of cases? Can EFD be used to verify information from other sources? Statistically driven case finding does not eliminate the need for traditional investigation, but can support more efficient investigations, reduce false positives, and identify productive prepay controls. EFD methods differ, as do interpretations of aberrant patterns found in claim and encounter data. This panel discussion examined the various methodologies and explored how each finds cases, how analysts evaluate the findings to determine if further investigation or analysis is warranted, and how cases are developed for administrative action or law enforcement.*

Speakers:

Patricia M. Connolly, Special Assistant US Attorney, District of Massachusetts, US Dept. of Justice (moderator)
Paul Deutsch, M.D., Empire Medicare Services
Eileen Guiney, EDS, Inc., Benefit Integrity Support Center
Paul A. Rustigian, Auditor, District of Massachusetts**,** US Department of Justice
David Sheridan, M.D., Palmetto Government Benefits Administrators

---

- Discussion at this session centered on a recent case, National Medical Care (NMC), which yielded the largest civil, criminal, and administrative health care settlement at the time, totaling $486 million,[8] the exclusion of three corporate entities from the Medicare program, and an eight-year corporate integrity agreement. NMC was the nation's largest provider of kidney dialysis services, with more than 600 facilities in 38 states, and generated about 60 percent of revenues from Medicare and Medicaid.[9] The investigation began in June 1994 with the filing of a *qui tam* (whistleblower) action and was fully resolved in January 2000, when the global criminal, civil, and administrative settlement was announced.

- Coordination, communication, cooperation, and commitment were the key ingredients leading to successful prosecution. Data analysis was one of six methods used to gather facts and prove the case, and was key to verifying allegations, focusing the scope of the investigation, and showing fraudulent billing practices. Data analysis permitted investigators to grasp the enormity of the case, better direct resources, and conduct the investigation more efficiently. Claims were the source of the data, from which investigators looked at types of claim (Medicare Part A or B), services claimed, paid and denied claims, and dates of service and volume of claims.

---

[8] The administrative settlement resulted in NMC's withdrawal of appeals seeking payment for more than $100 million in denied claims. The USAO's data analysis efforts thus focused on both paid and denied IDPN claims to facilitate the ultimate global – criminal, civil, and administrative – settlement.

[9] Medicare pays for dialysis services for beneficiaries of any age, provided an average of three to four times per week for an average of three to four hours per treatment. Medicare pays a composite rate to facilities for dialysis equipment, supplies, and services, but also pays separately for "ancillary" services, (e.g., certain laboratory blood tests, drugs and diagnostic tests)

- Employing a full-time consultant data analyst, the DOJ was able to test allegations and prioritize the government's theories. Data analysis was key to establishing a baseline from which to compare NMC's activities, and to identify spikes and patterns. The combination of data analysis with program expertise repeatedly proved invaluable. For example, data analysis revealed billing month after month for infusion pumps and poles, which was not reasonable or necessary because these pieces of equipment were available, at no cost, within the facility.

- Despite its critical importance, some difficulties arose in the analysis of HCFA data. For example, many claims had incomplete data fields, making it difficult to match Parts A and B data. Given the novelty of much of the analysis associated with the case, many of the weaknesses had not been recognized previously. HCFA has taken steps to address these issues.

- Possible considerations for future cases based on the NMC investigation and prosecution include:
  - When conducting analysis, it may be helpful to link related providers to get a more complete picture; each related provider may fall below the radar screen when viewed independently, but not when viewed globally;
  - Linking Parts A and B provides a more complete picture of a patient, facility, and physician.
  - If services do not appear out of line, you may want to look and see whether 100 percent of patients at one facility received the same diagnostic test on the same date of service.
  - Policy and data staffs should communicate. Investigators, medical personnel and policy staffs should understand how services are billed and should review actual claims data.

- The systematic medical model used to fight disease may be applied to combating health care fraud, waste, and abuse (FWA). In the disease model, the first step is identifying the disease organism and examining epidemiology or where/what it is striking. This is equivalent to detecting FWA, and determining where it is occurring. As epidemiologists must be sleuthful in their work, the FWA investigator does best approaching his task with a "criminal mind" in order to know what to look for and where to look for it. Next comes understanding the etiology, or underlying cause, of the disease, akin to drilling down, focusing, and analyzing the data. Such analysis leads to the development of treatment, which can be equated in the FWA example to collecting overpayments, referring fraud cases to law enforcement, and offering provider education. Understanding the cause of a disease and knowing where it strikes allows us to practice preventive medicine. In the FWA arena, this can be equated to developing new edits, educating providers, and continuing trending and other analyses, to ensure that behavior has changed and to prevent further "outbreaks."

- Hardware must have sufficient capacity to meet the data analysis needs. Furthermore, the successful analysis team is enhanced with individuals who have clinical knowledge as well as members with HCFA regulatory policy and practice knowledge.

- It is helpful to employ a variety of tools, data sources, and analysis techniques. Tools and techniques one contractor uses include BESS, which analyzes trends of carrier national performance and paid/denied claims, STARS, Access, SAS, Excel, Standard Query Language (SQL), and Shared System Reports (VMS). This contractor also utilizes an in-house developed tool that looks at providers' monthly incomes and several other types of information that offer an early opportunity to identify indications of fraud. Using SAS, the contractor creates daily calendars that can reveal the amount of time spent daily on each service billed. Postpayment utilization review permits the contractor to compare peer providers by procedure codes, showing gradations by standard deviation, while summing the standard deviations for all codes offers a glimpse at the whole picture for a provider.

- Several suggestions include:
  - Revisit old queries, examining trend results from multiple points in time to determine if there is consistency, if previously identified problems have been corrected, or if there are any new problems, trends, or spikes.
  - Analyze claims for new services and benefits to look for inappropriate usage. New policies may not be fully understood.
  - Define the appropriate universe, or the findings will be irrelevant.
  - Use visually effective reports and charts.

- Operated by one of HCFA's new Program Safeguard Contractors, the Benefit Integrity Support Center (BISC), will work closely with HCFA's carriers and FIs in the New England states to support data analysis capacity and provide specialized data analysis services. The BISC will integrate Part A and B data for all New England states (HCFA Region I), and additionally has purchased mapping software to match addresses and zipcodes. HCFA is also working on combining Parts A and B data in HCFA Region V.

- When cases referred to law enforcement go to trial, HCFA and the contractor are, in essence, also on trial. Everything the contractor did may be scrutinized, so contractors should seek to ensure that their practices and procedures can withstand such scrutiny. "Post-mortem" examinations of all aspects of a case should be conducted to help identify where changes in procedure may be needed.

- Communications with organizations should be bolstered wherever possible. One contractor, for example, has developed a payment safeguard steering committee combining Parts A, B, and durable medical equipment staff to coordinate efforts, and alert each other to cases being pursued. This contractor also maintains a computerized bulletin board to communicate fast-breaking news, such as a bankruptcy announcement.

- New and revised methods, paradigms, and processes of fraud detection and abuse detection should be considered.
    - One approach could be based on a disease management model, to examine what services would be typical and expected to be provided when a patient presents with various clinical conditions. An extension of this could be a "whole beneficiary analysis," involving the review of a beneficiary's entire claims history.
    - "Triangulate" findings to ensure that they stand up when examined through various "lenses" or approaches for analyzing data.
    - Y2K led many contractors to trend data on a monthly, rather than six-month, basis.
    - Denial patterns should be monitored closely to assess whether providers may be actively trying to test the system.
    - Conduct best case/worst cases analyses, not just comparisons to the mean.

Early Warning Tools: Data Mining and Neural Networks: *Data mining and neural networks are high speed, high volume technologies that approach real time analysis of claim and encounter data, searching for unexpected and suspicious patterns. These tools offer the promise of shining an early light on newly emerging scams, so pre-pay controls can be established and investigations triggered. But is there another side to the story? These tools are often very resource intensive and are not only costly, but also require significant expert staff support. This session not only looked at the exciting promise of these tools, but also discussed some of their limitations.*

Speakers:
Tom Moore, Jr., Consultant to McNeil Technologies, Inc (moderator)
Gene DeAngelo, HOPS International
Bill Stotesberry, Intelligent Technologies Corporation
Steve Biafore, HNC Insurance Solutions

- By some estimates, while the quantity of data in the world is roughly doubling every year, the amount of meaningful information is not keeping pace. Only computers with ever increasing capacity and speed can search vast quantities of data for patterns and relationships that can be called information. As health claim and encounter data have grown in volume and detail, so have the opportunities to learn about health systems performance through data analysis.

- Because we don't always know what is in the data, we don't always know how to frame the questions. Data mining searches may therefore be conducted with few, or no, prespecified criteria, instead letting the data itself lead us to the questions to ask. Data mining may, at first, produce only vague and incoherent patterns of utilization or cost, prompting the investigator to add criteria which explore subsets of the data.

- Data mining facilitates information retrieval from the "debris" of seemingly unrelated data. A predictive model of events may emerge, with unexpected sequences and quantities. Neural networks - typically software that "learns" to sort and classify - can improve the value of data mining output by rapidly finding suspicious links between events and persons, or at least aberrant behavior. Neural networks vary in architecture and function; there is no clear choice for health fraud and abuse discovery.

- What is a "predictive model" and why is it important to have one? Predictive models enable detection of aberrant activity without bias toward any particular set of known schemes. Their power comes from their ability to combine hundreds or thousands of complex inputs to form a fraud risk-score. Predictive models are used to protect over 85% of the nation's credit card businesses. Every health care entity leaves a trail of data, which, if understood in enough detail, may reveal suspicious patterns. Predictive models collect information including claim and encounter data, facility and provider information, licensing information, and patient demographics. The model identifies high-risk activity by finding inconsistent and aberrant behavior patterns.

- Quality and completeness of data, as with any detection method, is also an issue for predictive models. For example, incorrect or incomplete data in the prepaid systems may limit applicability of advanced fraud detection tools.

- The predictive model takes into account a complete web of activities of patients and providers to find patterns consistent with, or at significant variance from, what other comparable patients and providers are doing. The initial result is a rank ordered list of patterns that vary from the expected. The model is dynamic, looks globally to detect behavior indicative of potential fraud and abuse, and is capable of continually evolving to detect new fraud schemes, as opposed to static fraud detection measures that can quickly become ineffective.

- A predictive model yields an index of suspicion, or "fraud score." The system yields reasons for the user to drill down to the claim level, procedure level, or patient level to learn how the score was reached. The key to producing accurate models is ensuring that the inputs underlying the models capture the correct information. Predictive models alone and their output are not sufficient for developing cases for action. Their value lies in finding cases that would have gone undetected with standard query methods.

- Several pieces of business insight with respect to high-tech tools include:
  - data mining works only with a data warehouse or a similar data bed;
  - fraud, as revealed through data analysis, is dynamic, flexible and highly opportunistic;
  - fraudulent activity constitutes only a small percentage of all transactions;
  - subtle linkages are most critical and often are discoverable only after repeated data mining;
  - tools are often best suited to advanced users; data mining and related tools require expensive equipment and highly trained operators, not to mention experienced investigators to study the information;
  - investigative judgment is key;
  - not rule driven, but readily adaptable to rules;
  - useful for detecting obscure but suspicious behavior;

- Results generally are improved when using multiple data sources as inputs. If a model yields wrong results (false positives, or can't detect known fraud), the investigator corrects the analytic patterns or adjusts the criteria. Effective solutions most often integrate multiple approaches and tools to accommodate the dynamic nature of fraud.

- Network identification is a process that computes the measure of relationships between entities in the guise of a "dissimilarity index." Network identification can be used retrospectively to review top-ranked networks to determine legitimacy (identify potential cases of fraud), set benchmarks for the future, and review and test for changes over time.

Likewise, network identification can provide an early warning by identifying new networks and significant increases in rank, permitting real-time response including determining potential exposure, looking at past instances of abuse, and setting up program safeguards.

- To be useful to law enforcement as a part of case development, and for potential presentation to a jury, it is critical that any model or technique be easily justifiable and explainable. Output of high volume, high-speed search tools will typically require major analysis and testing before becoming a basis for action.

- Administratively, data mining can report providers and patients whose conduct requires immediate attention. Reimbursement rules may be drawn based on findings of the tools and investigations can be supported without sending signals to those suspected. Costs may not be justifiable, however, unless the new tools are applied to larger populations.

Nursing Homes -- Developing a Data Mining Project to Attack an Emerging Problem: *A discussion of one project designed to review existing data for indications of fraud, abuse or neglect by nursing homes arising from their failure to provide care for services paid for by the new prospective payment system. The project is intended to address the change from a fee-for-service compensation system to a flat rate prospective payment environment in which financial incentives for fraud may encourage the failure to care for program beneficiaries. The project will consider licensing and quality of care data as well as other existing sources of automated data in order to target for further investigation potentially inadequate care and other indicia of possible nursing home fraud. The data mining project is also intended to establish a means of testing allegations of nursing home abuse against readily available data bases for purposes of determining whether a pattern of misconduct exists at one or more facilities and to assemble available data to prove civil and criminal cases.*

Speakers:

Jack Barrett, Assistant U.S. Attorney, Central Dist. of California, U.S. Dept. of Justice (moderator)

Pete Burdette, Technical Director, Division of National Systems, Center for Medicaid and State Operations, HCFA

John Cronan, Inspector, Office of Inspector General, U.S. Dept. of Health and Human Services

David Oatway, President, Chesapeake Applied Technologies, Inc.

- Under the direction of a contractor, the U.S. Department of Justice is engaged in a nursing home data mining project that will relate facility resources to residents' needs. The project's objective is to build a model of existing nursing home data to detect patterns of resident abuse and neglect, as well as potential financial fraud and abuse, by combining and analyzing data sets to facilitate innovative analyses. One goal in particular is to derive summary and detail data about chain nursing facilities in comparison to a control group.

- There are several justifications for combining data sets in innovative ways. For example, any one data set may be manipulated by providers, such as via commercially available programs that make MDS (minimum data set) data consistent. Likewise, facilities may make special preparations in advance of quality inspection surveys, thereby skewing resulting data. Finally, all sources rely on provider honesty, which sometimes is lacking.

- Data sets used in these analyses include:
  - MDS data;
  - Enforcement data from OSCAR, HCFA's online survey, certification, and reporting system; and
  - Staff time measurements.

- There are no surprises in the use of these data sets. Providers are well aware of them, and enforcement data comes as the result of routine surveys.

- The MDS contains 505 data elements. Every resident is clinically assessed on admission, and their MDS report is then updated quarterly, as well as revised annually and whenever there is a change in the resident's condition. MDS is important:
  - clinically, as it presents a clinical picture of the resident and his or her health status change over time;
  - from a regulatory standpoint, because it is central to a data driven survey process; and
  - payment-wise, as it is factored in to the nursing home payment system.

- OSCAR contains information regarding nursing home ownership, complaint / enforcement results, and previous survey results. State survey agencies conduct the surveys, and enter data into OSCAR. There is generally a 60- to 90-day lag between an action, survey, etc., and data entry. OSCAR does not, however, contain detailed descriptions of deficiencies; rather, they are described using short generic "tags." Many enhancements to OSCAR are underway, including an examination of how to link it to a new provider enrollment and chain ownership system. Quality indicator reports are available on every facility at the state/HCFA level.

- Staff time measurement results were generated by assessing the minutes of care provided in selected facilities during staff time studies in 1995 and 1997. The numbers are not standards, just the best information presently available, and are generally accepted by the industry.

- Resource Utilization Groups (RUGs) are a composite measure used to group residents with similar resource utilization and clinical characteristics. Resources include time spent on care, non-rehabilitation ancillaries, general services, and capital expenses. Utilization is derived from time studies and the MDS data. Residents grouped in the highest RUGs require two or more hours of RN-provided care per 24-hour period, while residents grouped in lower RUGs require progressively lower levels of care.

- Ultimately the project will look at the RUG classification for each resident in a nursing home, and divide that by the amount of staff time resources available by staff type (i.e., RN, LPN) to yield a resource ratio that will permit a snapshot view of a facility. The model is derived so that a score of 1.00 equals appropriate staffing to provide good care, while scores less than 1.00 represent deficiencies and greater than 1.00 represents superior. Statistical models do not, of course, assure adequate or inadequate care delivery, but can offer a launching point for investigation. There are a number of advantages to using such an approach:
  - It normalizes data (using minutes of care, not dollars) to facilitate comparison;
  - It is difficult for providers to manipulate;
  - After extract from the RUG, data analysis can be conducted using desktop computers;
  - The data needed is routinely collected and stored; and

- After extract from the RUG, only summary data is used, mitigating privacy issues

- So far, programming has been started, arrangements are being made to receive MDS data from the states, and testing is ongoing using hypothetical nursing facility data sets. The results will be used in a number of ways. For example, an array of facilities in target chains will be compared with summary information from a control group. Facility profiling will pull data from several sources from facilities under suspicion for comparison to a control group.

- The Department of Health and Human Services' Office of Inspector General assists State Medicaid Fraud Control Units with nursing home investigations. When considering whether to open an investigation, the focus is generally on deficiencies that pertain to the medical care and safety of residents, as well as to how the facility has scored in previous surveys. OIG field offices act as liaisons to state fraud working groups, meet with surveyors, look at other facilities in chains to assess whether a problem may be endemic to the chain, and look at inpatient hospital records to ascertain whether admitted nursing home residents are suffering from pressure ulcers, malnutrition, dehydration, hip fractures or other signs of possible resident maltreatment or abuse.

- Nursing Home Compare, which may be found on the HCFA website at: www.hcfa.gov/medicaid/nhcomp.htm, is derived from OSCAR data, but there can be lags because states are not getting surveys to HCFA immediately.

- Nursing facilities are required to post in the facility a copy of the report from their most recent inspection. The report indicates how well the nursing home meets Federal health and safety requirements, as well as any deficiencies found at the time of the inspection. Deficiencies are rated on scope and severity, with scope indicating how often a certain problem occurs and severity indicating how seriously the problem impacts the health and safety of residents.

- In response to audience questions, panelists stated that OSCAR data is accessible to carriers and FIs, and that to access it one should first contact the applicable HCFA regional office. Also, MDS data is available on a national level.

Fraud in a Capitated Managed Care Environment -- State Activity: *What is fraud in the managed care environment and how do you detect it? What information is available and how information systems relate to the managed care environment. How to detect underserved populations in a managed care environment.*

Speakers:
John Krayniak, Director, Medicaid Fraud Control Unit, New Jersey (moderator)
Pete Francis, Director, Program Integrity, Arizona Health Care Cost Containment Systems
Lou Ann Gebhards, Director, Program Integrity, Kansas Medicaid Managed Care
Nelly Ryan, Director, Bureau of Managed Care, Illinois Department of Public Aid

---

- In the context of managed care, the locus of fraud is between provider and patient, as opposed to fee-for-service medicine where it rests on the claim between provider and payor. In managed care, fraud may be committed by the managed care organization (MCO) itself (against the governmentally funded health program, for example), or by network providers against the MCO. It is important to be cognizant of conflicting issues.

- Examples of fraud that may be committed by MCOs include:
  - Inappropriately adding names to enrollment lists;
  - "Cherry picking" by discriminating against potential enrollees who may be expected to require high levels of services;
  - Delaying assignments to primary care providers, or access to specialty care;
  - Failing to timely notify the payor when a member moves or dies;
  - Offering financial incentives to primary care practitioners (PCPs) to keep specialty costs low; or
  - Failing to maintain net worth, net reserves, or reinsurance requirements.

- MCOs themselves may be victimized by fraud, and they tend to report fraud to the state only in such cases. Generally, fraud schemes in which the MCO is victimized are committed by network providers in schemes including the PCP, including:
  - Avoiding treating patients through restrictive hours, and/or inaccessible location;
  - Accepting kickbacks from specialists to refer members;
  - Delaying notification of the MCO when a member moves or dies; or
  - Failing to refer members to specialists for medically necessary care.

- Capitated managed care payment systems may encourage underutilization, which is defined as knowingly failing to provide medical treatment that is either medically necessary or contractually required. In capitated systems, the provider receives a set rate per covered enrollee per month. This amount is intended to both cover the cost of any services provided, and yield the provider some level of income. Since the provider is paid whether a service is provided or not, the fewer services that are provided the more of the capitated payment the provider can keep. Conversely, fee-for-service systems may tend to promote overutilization.

- Elements of underutilization may include:
  - A pattern (as opposed to isolated incidents) of failing to provide all contractually required treatment, of failing to provide service at all, or not providing all medically necessary treatment;
  - Policies, procedures, or incentives that encourage or support underutilization;
  - Harming patients or placing them at risk;
  - Certain physician incentives (*i.e.,* performing fewer services but getting the same amount of money, or bonuses for not referring patients to specialists or ancillary services)

- Methods of detecting and proving underutilization often involve looking for patterns of behavior. Possible proof may be found in documents, analysis, and testimony. For example, underutilization may be supported by analysis of certain information, such as:
  - Comparison of utilization to other similar providers.
  - Comparison of a providers' utilization under managed care with their utilization under
  - Comparison of services provided for the same patient before and after enrollment in managed care.
  - Evidence that a provider restricted office hours or discouraged the patient from coming to the office (*i.e.,* "I can get to you in six months," or "That sounds pretty bad, you should go to the E.R.")
  - Data suggesting an increase in emergency department utilization, or that the provider has transmitted false encounter data.

- It is beneficial if all contract terms are clear, concise, and unambiguous with respect to expectations and performance, as well as sanctions for poor or nonperformance. Fraud and abuse may be more likely to be prevented with the following measures:
  - A strong contract;
  - Ongoing oversight and monitoring;
  - Ongoing collaboration and problem solving with MCOs;
  - Ongoing collaboration with stakeholders and partners; and
  - Client (State Medicaid Agency) access to the Department (of Health or equivalent).

- It is also helpful for MCO contract provisions to address:
  - Whether to mandate encounter data;
  - Whether to mandate recovery of overpayments; and
  - Job requirements of the MCO program integrity chief, (the DHHS/OIG compliance guidelines serve as a prototype for this position, suggesting it be a high-level official who may exercise independent authority, and who has direct access to the MCO's governing body, CEO, senior management, and legal counsel).

- Contract monitoring is often vital to ensuring MCOs' operational and technical

compliance, as well as quality assurance. To illustrate, officials in one state meet quarterly with each MCO to review all aspects of operations, including meetings with the MCO's quality assurance staff, any behavioral health managed care subcontractors, and the systems unit staff to ensure updates on data issues. Equally important is ongoing collaboration with other stakeholders, advocates, and partners, the latter including HCFA, the State Insurance Department, and other state agencies. In Illinois, members have access to report complaints to the Department via a toll-free telephone hotline, the mail, their health benefits representative, or through reports to Department staff. Calls that require intervention, review, or investigation are documented as complaints, and are tracked via a database that allows for monitoring of patterns or trends. The Department also has conducted annual consumer satisfaction surveys.

- Just two of 102 counties in this state participate in a voluntary Medicaid managed care program. Of seven participating MCOs, five are private HMOs and two are nonprofit, provider sponsored managed care community networks (MCCNs). This represents a reduction from 14 MCOs, which resulted from MCOs consolidating, merging or going out of business. The state considered imposing mandatory managed care, but did not. As of June 2000, the state's Medicaid enrolled population in managed care exceeded 136,000.

- Marketing representatives in the state are credentialed by the MCOs. Requirements to be approved as marketing representatives include that the candidate:
  - Has no felony conviction in the last 10 years;
  - Was not discharged, or did not resign, in the last 12 months for prohibited marketing practices;
  - Completed Department-approved training;
  - Has no other association with a different MCO;
  - Is a provider of medical services; and
  - Holds a valid license or certification from the Department of Insurance.

- The state health agency maintains an historical log of all current and previous marketing representatives, and identifies representatives that have been suspended, terminated, barred, or who are currently under investigation for engaging in prohibited marketing practices or other misconduct related to marketing. Prior approval is required for marketing representative training manuals, marketing materials, promotions, etc., and the agency conducts unnanounced observation of marketing representative training sessions. Ten enrollment marketers have been prosecuted for contract violations and not permitted to engage in enrollment activities. The state health agency cooperates closely with the state's Office of Inspector General (OIG), holding monthly meetings and referring to them all marketing complaints. Fraud cases substantiated by the OIG are referred to the State Attorney General's office.

- Additionally, detection of potential marketing fraud and abuse occurs via:
  - Calls to a hotline;

- Self-reporting of incidents of fraud;
- Reporting of suspected fraud by competitors;
- Ongoing review of enrollment and disenrollment forms; and
- Statistical analysis of reasons for disenrollment.

- MCOs are required to have approved grievance procedures, which outline the process for handling grievances arising from both administrative as well as clinical issues. Members may appeal decisions to the state health agency. On a quarterly basis, MCOs must report grievances received and resolutions to the agency.

- The state attempts to capture encounter data from MCOs to track services such as prenatal and behavioral health services utilization. However, the State lacks legal authority to require encounter data submission, and officials have found that providers are frequently unwilling to give data to the MCOs, while hospitals have no incentive to provide data. As such, the state reports that it receives only about 40 percent to 50 percent of encounter data.

- All of a second state's Medicaid population is in managed care. In the 1980s it was assumed that managed care would solve the fraud problem, when in fact it has actually compounded it. One example was a case in which an MCO subcontracted with another organization to provide care for 1600 of the MCO's members. The subcontractor used the money to pay other debts and subsequently went bankrupt, upon which the MCO reported this as fraud to the state and its members were reassigned.

- Three implications of managed care are that:
  1. Managed care controls must be different than those for FFS, as traditional controls are not sufficient;
  2. All administrative functions of the Medicaid state agency should be designed with fraud control as a goal; and
  3. Significant responsibilities and duties assigned by law, administrative rules, and/or contract provisions to MCOs and providers facilitate program integrity efforts.

- Responsibilities of the MCO in this second state include:
  - Developing and implementing a fraud and abuse control plan, and a compliance plan;
  - Maintaining effective detection systems to see that providers / subcontractors are not committing fraud;
  - Having effective reporting protocols;
  - Training employees in the compliance program, how to recognize potential fraud, and how to properly respond; and
  - Understanding that they must cooperate with law enforcement and PI units.

- Program integrity units in the state:
  - Monitor contract compliance;
  - Conduct program audits of "vulnerable" services, such as prescription drugs, dialysis,

and medical transportation;
- Conduct quality assurance oversight;
- Provide financial oversight;
- Furnish MCO and provider training;
- Develop contract provisions, *i.e.* for fraud and abuse encounter data adjustments or fraud and abuse overpayment recovery;
- Analyze encounter data;
- Facilitate agency-wide coordination; and
- Conduct preliminary investigations.

- The state conducts quarterly fraud and abuse meetings with the MCO fraud and abuse staff, the state MFCU, and private providers. State officials always try to present a training case example at each meeting. The state also sends its staff out to other providers for training on how to detect managed care fraud.

- Possible implications for technology with respect to managed care fraud are that:
  - Current technology may be inadequate to support PI units operating in a managed care environment;
  - State agencies may need decision support systems and more sophisticated statistical and analytic applications; and
  - MCOs may need new and better technology.

- A third state's experience has shown that selling the physician community on managed care has proved difficult. This state's managed care experience dates to 1995 when there were three MCOs. Two dropped out after three years, leaving one remaining plan, which went bankrupt in May 1999. A fourth plan assumed the contract of the bankrupt plan. The capitated plan is limited to an HMO in two metropolitan areas, into which mothers and young children were the first enrollees. A primary care case management (PCCM) plan operates in the western part of the state. As of May 2000, the state's PCCM and Medicaid managed care systems' total enrollment exceeded 115,000.

- The state's fiscal agent uses a team of nurses and social workers to address complaints for the HealthConnect PCCM program. Complaints from MCO beneficiaries are received either by the MCO directly or by the HealthConnect team but are referred back to the MCO for resolution. Enrollee complaints typically have dealt more with quality issues, including underutilization, than with financial matters. A professional review organization (PRO) conducts external quality of care reviews.

- The state Medicaid Agency's contracts require a compliance plan, written in collaboration with the state's MFCU. The MFCU employs a decision support system implemented with the most recent Medicaid Management Information System contract in 1996.

- The state's contract provisions require MCOs to monitor complaints and grievances they

receive and to report them to the state. Complaints against MCOs have been low when compared against the FFS system, however the definition of "complaint" versus "inquiry" bears clarification. A complaint typically heard from Medicaid beneficiaries is that they are not aware who PCP is, because providers often fail to print cards or furnish them to beneficiaries. Beneficiary reports of difficulty getting to their PCP leads to questions as to whether the provider network is adequate.

- To date, this state has reported no fraud prosecutions, and just one fraud referral involving Medicaid managed care. The state conducts credentialing reviews in conjunction with HCFA requirements, and the external quality review organization (EQRO) conducts these reviews as well. Although its contracts with Medicaid MCOs allow the state to access contracts that the MCOs enter into with plan providers, the state has not sought such access. However, HCFA personnel, accompanied by staff from the state, do review the MCOs' credentialing of their providers.

Medicaid and Electronic Fraud Detection: *What states are doing with electronic fraud detection, and what more they would like to accomplish with it.*

Speakers:

Carlis Faler, Program Integrity Director, Mississippi Division of Medicaid (moderator)
Cheryl Brady, Branch Chief, Kentucky Department for Medicaid Services
Aurora LeBrun, Associate Commissioner, Texas Health and Human Services Commission, Office of Investigations and Enforcement
Robert "Bo" Nowell, Asst. Director, Program Integrity, North Carolina Division of Medical Services
John Owens, Chief, Medicaid Program Integrity, Office of Inspector General, Agency for Health Care Administration, Florida

---

- One state's Medicaid program spends about $15 billion annually. A fragmented claims processing system spread across multiple agencies did not provide the ability to conduct an analysis of a provider's participation in multiple programs and across agency lines to develop a comprehensive case investigation. As directed by its legislature, this state implemented a system known as the Medicaid Fraud and Abuse Detection System (MFADS) in late 1997. With MFADS, the state became the first to implement neural and learning technology for the detection of fraud and abuse in health and human services programs.

- MFADS integrates both historical and current data stored in the various processing systems into a single data repository. Through intelligent technology, the system analyzes Medicaid provider and recipient participation in multiple programs across agency lines, identifying potentially aberrant practices and suspicious patterns. New fraud and abuse schemes can continually be anticipated and identified because the neural network technology lets the system "learn" and recognize possible new fraud and abuse patterns. Investigative staff using online desktop tools connected to the system conduct focused research and review efforts, and comprehensive case development.

- The MFADS technology has:
  - Made possible the recovery of large overpayments;
  - Identified fraudulent and other inappropriate claims payments;
  - Identified Medicaid policies or procedures prone to fraud or abuse;
  - Enabled the imposition of civil and punitive sanctions;
  - Led to the recovery of almost $5 million in 30 months and to the identification of almost $9 million for recovery;
  - Been responsible for almost $2 million in savings to the Medicaid program; and
  - Produced projected efficiency gains averaging 125 percent of project costs as of February 29, 2000.

- A second state's Medicaid agency employed a contingent-fee recovery contract to identify

and recover Medicaid payments determined to be potentially abusive, fraudulent, or otherwise inappropriate. In general, the state was able to conclude that the vast majority of Medicaid providers in the state were honest and ethical professionals, however there were some cases of inappropriate billing through either honest mistakes or intentional deceit.

- The state fiscal agent, provided the contractor with five years of paid claims and adjustments data, along with all billing instructions, program manuals, provider letters, regulations, and other relevant material in effect during the five-year period. Algorithms and detection criteria were crafted to identify billing combinations that should not occur or be paid. Computer runs produced subsets of questionable claims by provider type, and occasionally different subsets among the same provider type, to account for coverage changes occurring during the course of the five years worth of data.

- Each subset run was forwarded to the state's Department for Medicaid Services for a validation review. When the contractor's conclusions were deemed correct, they were presented to a Review Board consisting of personnel from the U.S. Attorney's Office, the State MFCU, the Cabinet for Health Services Office of the General Counsel, the Cabinet for Health Services Office of Inspector General, and DHHS/OIG. Review Board meetings were held to obtain input from law enforcement agencies, and to assess the potential for investigation. Where appropriate, the contractor initiated or deferred recovery efforts in coordination with law enforcement.

- As part of an incremental approach toward an agency-wide solution, a third state's Medicaid program embarked on a major upgrade of its electronic fraud and abuse detection system (FADS) in September 1999 when it contracted for two software products, support services, and the required hardware. Necessary precursors to this upgrade came in 1998, with the addition of a PC based local area network (LAN) system, a data warehouse, and a claims imaging system. The PC-LAN system was necessary as a platform and stepping stone for the data warehouse and the FADS, and led to significantly increased productivity and recoveries. The data warehouse contains three years of claims data and is the foundation for the FADS. The program also shifted from microfiching claims to claims imaging, allowing claims to be pulled up on staff PCs.

- The state next purchased two fraud and abuse oriented software products, a PC-based client server SURs-type system, and a fraud and abuse detection software tool. Critical factors were for the products to:
  - work off the data warehouse;
  - provide simple user interface for all PI staff;
  - allow drill-to-detail and export data to spreadsheet capabilities; and
  - be something that state staff would use as an investigative tool.

- Conversion of the state's MMIS legacy system, which lacked claim detail information online, to a browser-based system with the addition of a claim detail database is in process.

While the old system required ordering claim histories that frequently took at least a week to arrive and involved significant human processing, the new browser based system will have features making the system both easier and quicker to use, providing results from five to nine days faster than the old system, and enabling staff to answer provider complaints more quickly.

- The state added several additional features to enhance investigations and improve customer service, including:
  - A software package that permits reports to be placed on web access where they can be manipulated and exported for use. Remittance Advice and Status Reports and Paid in Full reports will be loaded initially followed by cost report summaries;
  - A provider call tracking system, whereby provider calls are logged into a tracking database that sorts information about the call and the caller. Frequently asked questions (FAQs) get catalogued to assure the same question always gets the same response, cutting down on "answer shopping." FAQs become part of future training. Staff can avoid duplicative research, and investigative staff will benefit from knowing if a provider was provided incorrect information or ever contacted the agency or fiscal agent; and
  - Online research and reference material, including CPT and ICD9 codes, provider manuals, and other reference information, will be available for all staff. Research will be faster and easier, and online resources save the time and clerical work otherwise necessary to maintain paper-based materials.

- In a fourth state, a contractor is performing program integrity work in the area of prescription drug benefits. The contractor is auditing pharmacies it identifies, and recovering any identified overpayments. Contingency fee contracts can give rise to a number of issues, however, including whether the contingency fee contractor is responsible for identifying potential fraud or abuse, or just making recoveries.

Fraud in a Capitated Managed Care Environment -- Federal Activity: *What is fraud in the managed care environment and how do you detect it? What can you do with encounter data? What information is available and how information system related to the managed care environment. How to detect underserved populations in a managed care environment.*

Speakers:

Dan Anderson, Senior Counsel, Civil Division, US Department of Justice (moderator)
Barbara Bisno, Assistant US Attorney, Civil Division, Southern District of Florida, US Department of Justice
Craig Briggs, Office of Audit Services, Office of Inspector General, US Dept. of Health and Human Services
Cynthia Moreno, Health Care Financing Administration
Rose Sabo, Director of Program Integrity, Tricare, US Department of Defense
Linda A. Wawzenski, Deputy Chief, Northern District of Illinois, US Department of Justice

---

- Sixteen percent of Medicare beneficiaries and 50 percent of Medicaid beneficiaries are enrolled in MCOs.

- A number of *qui tam* relators' attorneys whose efforts were focused on tobacco litigation recently have turned their attention to managed care, raising expectations of increased litigation in this arena over time. Common bases for *qui tam* actions include:
  - Plans misrepresenting the nature of their patient population;
  - Forced disenrollments;
  - Plans failing to provide adequate provider networks; and
  - Plans "cherry picking," or using a variety of mechanisms to restrict enrollment to healthy individuals.

- TRICARE, the US military's health plan, maintains a national database called the Care Detail Information System, or CDIS. The CDIS is able to track how much care beneficiaries are receiving, how much care providers are providing, and how contractors are handling claims. Storing more than 90 million claims, the system offers a nonintrusive way to evaluate allegations and suspicions, reducing the need for audits. CDIS can identify abnormal billing patterns, such as billing for more hours than are in a day. CDIS has been used in a number of practical applications, including:
  - Investigating allegations of fraud overseas, where a massive provider/beneficiary fraud ring was uncovered that included billing from nonexistent facilities;
  - "Ghost provider" scams, in which fraudulent providers made claims using legitimate beneficiary names and having checks sent to a Post Office box, only to disappear when the first claim was denied; and
  - Helping to track down and warn patients victimized by a California physician who had watered down immunizations.

- HCFA maintains a presence to ensure the integrity of Medicare managed care operations through a tiered monitoring program that includes routine monitoring visits to the managed care organization's facilities, focused monitoring visits, and intensive enforcement visits. Routine monitoring visits include on- and offsite work conducted by HCFA's regional offices after a contract is awarded, and biennially thereafter. Focused monitoring visits, which may occur at any time, are conducted in response to problems, which may come to light from such things as complaints and identification of issues during routine visits. Intensive enforcement visits follow enforcement action(s) and may be focused or cover an MCO's entire Medicare operation.

- Problematic areas in Medicare managed care operations have been in the areas of claims processing, enrollments/disenrollments, appeals/grievances, and membership reconciliation.

- HCFA can impose intermediate sanctions on MCOs for infractions including the following:
  - Misrepresentation to HCFA or a beneficiary
  - Interference with practitioner advice to enrollees (gag rules)
  - Failure to enforce private fee-for-service balanced billing
  - Practices that may discourage enrollment
  - Charging in excess of the allowed premium
  - Contract failures
  - Violation of prompt payment

- HCFA is developing a managed care information system for monitoring and feedback purposes. The system will yield standardized monitoring reports, and data analysis will enable HCFA to focus on problematic areas.

- Mechanisms in place in one state for MCO fraud and abuse prevention include a strong contract, ongoing oversight and monitoring, and ongoing collaboration and problem solving with MCOs. Contract monitoring entails ensuring operational compliance, quality assurance, and technical compliance.

- This state particularly emphasizes monitoring marketing activities. Marketing representatives must be credentialed by the MCOs. The state agency maintains an historical log of all current and previous marketing representatives, including a registry of all representatives suspended, barred, or under investigation for engaging in prohibited marketing practices. As do a number of state Medicaid programs, this state requires prior approval for the marketing training manual, marketing material, and promotions, and there is unannounced observation of marketing representatives training sessions.

- MCOs in this state are required to have approved grievance procedures that outline processes for handling administrative and clinical issues. MCO members may appeal decisions to the state agency, while quarterly reporting of grievances and resolutions to the

state agency is required. Ten marketers were recently prosecuted, much of this effort stemming from close cooperation between the state agency and the OIG. Meetings are held monthly, and fraud cases substantiated by the OIG are referred to the state Attorney General's office.

- Complaints are received through many means, including via a hotline, from health benefits representatives, by reports to state agency staff, through the mail, from MCO competitors, via self-reporting, from ongoing review of enrollment and disenrollment forms, and from statistical analyses of reasons for disenrollment. Calls requiring intervention, review, or investigation are logged as complaints and tracked via a database that allows for monitoring of patterns or trends.

Prepay and Postpay Systems: *Distinctions between prepay and postpay systems and how we can move towards a more proactive prepay stance. Can new fraud and abuse patterns be effectively detected through prepay systems? Can electronic fraud and abuse detection systems supplement efforts to educate honest providers making unintentional coding errors?*
Speakers:
John Stewart, Statistician, Program Integrity Group, HCFA (moderator)
Paul Deutsch, M.D., Empire Medicare Services
Jeff Harrison, National Heritage Insurance Corporation
Arthur Lehrer, VIPS Healthcare Information Solutions
David Sheridan, M.D., Palmetto Government Benefits Administrators

---

- The fraud detection paradigm can be viewed as a cycle in which retrospective review and analysis of paid and denied claims leads to determination of fraud schemes, which leads to the development of screens, leading in turn to the development of prepay edits. This cycle continues as new fraud schemes evolve.

- Denying claims on prepayment review yields from five to 15 times more savings than attempting to recover overpayments on postpayment review. A Medicare contractor adopted a requirement for prepayment review of medical records for psychiatric services when it found billing for psychiatric services in the area it served to be 10 times higher than the national norm. In another example, the contractor saved $6 million by instituting a pre-pay denial policy for 160 providers who were billing the top 100 beneficiaries.

- It is important to consider how prepayment review systems will be integrated with the claims processing system. Prepay review systems must determine on the fly what will be paid and how values compare to norms, act on any rules established for a provider, and be able to stop payment before it is made. Every action that a prepay system takes must be documented with an audit trail.

- Because standard tools and technologies tend to detect only the "tip of the iceberg," it would be beneficial to run Part A and B data sources through sophisticated analytical modeling. Many patterns are subtle and may be detected only with advanced models. But as a corollary, good tools demand good people, for they are only as effective as the questions asked.

- To facilitate the efforts of law enforcement, documentary evidence for cases, including medical records, may be sent to law enforcement via CD-ROM.

- HCFA rules require that Medicare contractors provide 48-hour advance notice prior to a site visit. One contractor has found the use of portable high speed scanning technology to scan medical records very helpful when conducted site visits.

- There are a number of instances in which HCFA and many of its contractors do not contribute to their own cause of combating fraud and abuse. For example, many types of Medicare contractors' systems lack any type of interface across lines of business, significantly hampering analytic capabilities. HCFA's National Claims History file does not retain Part A denials, significant because analyzing denials can yield as much information as analyzing paid claims. Also, the referring provider field is not retained.

- In combating fraud, the question is more important than the answer. The wrong question will not assist you in correcting abuse, regardless of the power of the analytic tool. As important as any electronic tool may be, the original neural net - the analytic staff - is just as important, if not more so.

<u>Cross-Claims Analysis: Home Health Agencies</u>: *A panel discussion on completed and future Cross Claims Analysis projects comparing home health agency data between Parts A and B. This discussion covered an initially labor-intensive project reviewing referrals that involved the FI and carrier for one state, the post-prospective pay era where home health agencies may be attempting to shift claims to Part B, and a discussion of the possible uses of an electronic comparative analysis tool in the home health arena (i.e., comparing care plan oversight data with payment data).*

Speakers:

Larry Young, Health Insurance Analyst, Special Initiatives and Data Management Unit, Health Care Financing Administration, Region VI (moderator)

Alyce Embree, Fraud Unit, Palmetto GBA

Charles Haley, M.D., Associate Medicare Medical Director, Trailblazers Health Enterprises, Inc.

- Data mining is the process of extracting meaningful information from large databases. Once extracted, information can be analyzed to reveal hidden patterns, trends, relationships and correlations among data.

- Data mining can uncover patterns associated with past fraudulent behavior in order to identify future fraudulent usage and trends. It can profile common usage scenarios and flag new or different patterns for further investigations.

- Data analysis can:
  - Set investigative leads;
  - Define investigative strategies;
  - Prioritize investigative efforts;
  - Identify fraudulent behavior and trends;
  - Profile common fraud scenarios and flag new or different patterns for further
  - Investigation;
  - Discourage future fraudulent behavior;
  - Save time and investigative resources;
  - Reveal irregular and fraudulent billing and claim patterns;
  - Reveal patient/client sharing between providers, hospitals, clinics and attorneys, that may indicate a bribe, kickback or referral scheme;
  - Identify and qualify case subjects, witnesses and victims; and
  - Increase probability of prosecution, conviction and/or restitution of stolen assets.

- Two Medicare contractors engaged in a collaborative effort, with participants located in three states. At the time of this initial project, the participants had no way to communicate electronically. All transfers of data were done on disk, through the mail. Much of what was done by hand in the initial investigation now can be done by E-mailing data files and using software packages such as STARS.

- One contractor analyzed Medicare Part A home health data and sent to two states information pertaining to the top 50 providers operating in each state. Both states examined relevant Part B data and refined their respective lists to less than ten providers each. The remainder of this case discussion addresses details of the subsequent investigation in one of those two states.

- The contractor ranked all home health agencies (HHAs) from this particular state based on two variables, (1) average reimbursement per patient, and (2) average visits per patient. These rankings were combined and the top 50 agencies were identified as needing further investigation.

- These were referred to the second Medicare contractor, who through additional data analysis refined the list of potentially suspect providers to 10 HHAs and physicians.

- The second contractor identified the referring physician for each selected home health agency. All Part B claims for the referring physician were examined.
  - The proportion of patients with any Care Plan Oversight (CPO) claimed was calculated.
  - The proportion of HHA dollars accounted for by physician was calculated.
  - The physician's Part B billings were examined.
  - The final selection of HHAs and physicians took several factors into consideration:
    - Evidence that one physician accounted for the majority of an HHA's income; (In one instance, one physician accounted for 68 percent of one agency's income.)
    - Either high or low Part B dollars; (For example, one physician accounted for 65 percent of one agency's income, while at the same time the physician had almost no Part B income) and
    - Area of state.

- A field investigation was based on the data analysis and consisted of:
  - Interviewing 149 beneficiaries to determine their homebound status and the medical necessity of the services billed by the home health agencies.
  - Interviewing 25 physicians to determine whether they understood the requirements for beneficiaries to receive home health services.
  - Physician interviews were also used to identify financial or business relationships between the physician and home health agency, and to assess the physicians' procedures for monitoring the patients' conditions.

- The results of the investigation included:
  - A total of 761 claims were reviewed, involving 12,367 services;
  - Of the 12,367 services reviewed, 7,266, or 59%, were supported with documentation obtained from the home health agencies and physician offices. The remaining 41% of

services billed were denied for one or more of the following reasons:

- Beneficiaries did not meet the homebound criteria established by Medicare guidelines;
- Agency personnel provided services that were not medically necessary, or the beneficiary had no qualifying skilled health care need;
- Agency billed for services that were deemed stable/chronic/custodial care.
- Agency billed for services not documented in the medical records;
- Agency billed for services rendered to immediate family members of one of the agency's owners; and
- Identification of overpayments in excess of $300,00.

- The majority of the physicians interviewed appeared to have a clear understanding of home health requirements, including the homebound requirements. No physicians were identified as having a financial ownership interest in the agencies, but one physician was identified as an HHA's medical director and was the top referring physician for that agency. The physician had no office space within the HHA, but made periodic home visits with the agency administrator. Beneficiaries said this physician was not their primary care physician, and there were indications that a kickback arrangement might have existed between the HHA and the physician.

- The two Medicare contractors are now under the same corporate umbrella, which may facilitate future exchanges of data and other cooperative investigations. In addition, one contractor has been engaged in loading all HHA payments into STARS, a fraud detection software program.

- Future ideas for investigation include:
  - Once a physician(s) with a high percentage of referrals is/are identified, all HHA billings in which he/she/they are listed as the referring physician(s) should be examined.
  - These charges, regardless of the HHA, should be plotted over time by HHA and physician. Shifts in referral patterns between HHAs can then be identified, as well as those HHAs associated with the targeted physicians.

State Medicaid Efforts: *Presentations on two state payment accuracy measurement studies,*[10] *Texas' "A Health Care Claims Study," and Illinois' "Payment Accuracy Review of the Illinois Medical Assistance Program."*

Speakers:

Rose Crum-Johnson, Southern Consortium Administrator, HCFA (moderator)

Aurora LeBrun, Associate Commissioner, Texas Health and Human Services, Office of Investigations and Enforcement

Robb Miller, Inspector General, Illinois Department of Public Aid (IDPA)

- The Illinois Office of Inspector General conducted a study of Medicaid payment accuracy in 1998. The study was not conducted to establish a "fraud rate"; the state Inspector General conducting the study conceded that establishing a fraud rate may not even be possible.[11] The study examined a statistically valid, stratified random sample of 599 medical services adjudicated, processed, and approved for payment during January 1998. The universe of services was stratified as follows prior to sampling:
  - physicians and pharmacy services;
  - inpatient hospital and hospice services, and
  - all other types of services.

- A four-step review process was used that involved client interviews, medical records review, contextual claims review looking at other claims seven days before and after the service in question, and a final analysis from an expert review panel. Each service was categorized either as having been paid correctly or in error. Questions of medical necessity were not considered an error factor. The study found a 95 percent payment accuracy rate. Conducting the study was labor intensive, calling for 14,000 staff hours in six months. The study was also expensive, with direct costs totaling $400,000.

- The study provided much needed empirical evidence and established a baseline for future measurement efforts. Additionally, the study helped validate much of the state's extant program integrity efforts. For example, 28 of 29 suspect noninstitutional providers identified by the study were already under review. As a result of the study, requests for proposals were issued to address particular issues identified with regard to nonemergency transportation and procedure coding review, and procedures tightened for monitoring newly enrolled providers.

---

[10] Although not presented during this session, the Kansas Medical Policy Department, Social & Rehabilitation Services, published another payment accuracy report, *Payment Accuracy Review of the Kansas Medical Assistance Program*, in April 2000. The study examined a sample of 600 fee-for-service claims paid during March 1999. Targeting four categories of claims including pharmacy; inpatient hospital; home and community-based services; and all others, the overall payment accuracy rate was calculated at 76 percent, with a margin of error of 9 percent. (Report at Page 9).

[11] Illinois Department of Public Aid, *Payment Accuracy Review of the Illinois Medical Assistance Program: A Blueprint for Continued Improvement*, August 1998 at page 3.

- Nonemergency transportation was the area identified as the single greatest concern. Of $37.2 million spent for nonemergency transportation services included in the study's universe, $11.55 million, or 31 percent, was estimated to be in error. Nonemergency transportation poses particularly troublesome issues because it is one of the few services for which beneficiaries may defraud the system as easily as providers.

- In 1997, another state's legislature mandated a health care claims study in an effort to measure fraud in the state Medicaid system. The state comptroller and auditor were responsible for producing the study, which was not published in final form due to methodological problems that arose. Estimates of fraud rates at that time ranged from 2 percent (by management) to 40 percent (by Public Broadcasting System's *Frontline* series).

- The unpublished study results indicated that between 6 percent and 6.5 percent of the spending on acute care claims was lost to errors or overpayments, for a loss of between $143 million and $162 million annually. The study looked only at acute care claims paid by the states Medicaid contractor. The universe of claims was 32 million, submitted by 164,000 providers. The measure of analysis was services provided on one patient day, with the study examining a total of 700 patient days. The study methodology included client interviews, conducted either face to face or by telephone, using standard questionnaires tailored to the type of service (i.e., durable medical equipment, transportation, hospital, etc.). All claims for each patient day within each service category were used to calculate an estimated average claim amount for each service category.

- A contextual data analysis was conducted, from which an assessment of potential overpayments was made, looking at such factors as whether:
  - Services were not rendered;
  - There was sufficient documentation;
  - Services were related to a prior or ongoing condition;
  - Procedures were inconsistent with diagnosis, or treatment inappropriate to condition;
  - Multiple diagnoses were inconsistent;
  - Claims were incorrectly coded;
  - Services were unbundled;
  - There were duplicative services; and/or
  - There was a consistent trend in ongoing services.

- Medical records were requested when the interviews suggested discrepancies. Providers were given three opportunities to send records, with failure to comply leading to payments being recouped. Seventy-four percent of medical records were received.

Return on Investment Issues / The State of the Surveillance and Utilization Review System (SURS): *High costs of technology are colliding with limited public resources and political resistance to new investments. How can the economic value of electronic fraud detection (EFD) be measured? Can the costs be justified? Is return on investment important when considering fraud and abuse prevention? Or should other public interests affect investment decisions? This panel will discuss criteria for measuring the value of investing in EFD, including social, political, and economic criteria. Discussion will also look at the state of the SURS, and how to fund technology that will enhance the SURS, not simply upgrade them.*

Speakers:

Tom Moore, Jr., Consultant to McNeil Technologies, Inc. (moderator)

John T. Christian, Senior Business Process Analyst, U.S. General Accounting Office

Robert "Bo" Nowell, Assistant Director, Program Integrity, North Carolina Division of Medical Services

---

- The U.S. General Accounting Office (GAO) has produced an assessment framework to help guide Federal agencies in guiding and managing their IT investments. Annual federal spending on IT investments has grown to nearly $38 billion, representing investments in telecommunications and networks, new operating systems and software, continued support and operations of existing infrastructure, and data centers, all of which directly affect agencies' abilities to achieve improvements in mission performance, management decision-making and oversight, and operational efficiencies.

- The investment management process is comprised of three phases: the select, control, and evaluate (S/C/E) phases. In the select phase, the costs and benefits of all available projects are assessed and the optimal portfolio of projects is selected. During the control phase, the portfolio is monitored and corrective action is applied where needed. In the evaluate phase, implemented projects are reviewed to assure that they are producing the benefits expected and adjustments are made where appropriate. All stages may be underway at once with respect to different projects at different stages of their life cycle.

- Although the GAO found some sort of IT investment management process in nearly all Federal agencies, none had implemented stable processes to address all three phases of the S/C/E approach. The GAO identified that the S/C/E approach has shortcomings, including that it:
  - fails to provide a comprehensive discussion of the organizational processes required to build a stable IT investment management organization;
  - does not identify those organizational prerequisites that must be in place for the process to remain robust and stable; and
  - does not address the need for continuous improvement and clearly defined requisites for moving from the current investment management state to a more advanced state.

- Thus, the GAO refines the process by embedding the IT investment management process within a five-stage maturity framework that explicitly describes the organizational processes required to carry out good investment management. As organizations improve their IT investment management capabilities, their capability and process maturity increases. Each stage, with the exception of the first, is composed of critical processes that must be implemented and institutionalized for the organization to satisfy the requirement of the maturity stage.

- One speaker offered a case study on return on investment from upgrades to the state's SURS. Having just added a local area network and a new data warehouse, the state's 18-year-old RAMS II SURS still worked, but would have required substantial modification, at an estimated cost of $2.65 million, to adapt it to new coding procedures and to make it Y2K compatible. Facing these costs just to renovate an antiquated system, the state elected instead to spend $3.9 million over the course of three years for both a new SURS and fraud and abuse investigation software.

- Upgraded SURS can produce both tangible and intangible returns on investment, including:
  - Recoveries resulting from investigations developed from SURS leads can be tracked;
  - Cases referred to the MFCU and dollars returned by the MFCU as a result of SURS can be tracked;
  - Support provided to the MFCU in legal actions using SURS data, to illustrate the aberrant billing patterns of providers in relation to their peers, can make prosecutions more successful;
  - Savings from changes made to medical policies as a result of the identification of problems related to specific services and codes;
  - Savings resulting from the addition or revision of prepayment MMIS audits and edits; and
  - Savings from intervention made when aberrant patterns are discovered and the provider is notified of investigation or educated on their problem area.

- Modernizing a SURS, and the related business process re-engineering, creates a new dynamic among agency staff. For example, older SURS often were paper driven, and research consisted of spending hours looking through green bar paper or microfiche. Obtaining results could take weeks or months, so by the time problem providers were identified, the program may already have lost significant amounts of money. Newer SUR subsystems offer real time processing that can yield reports magnitudes of order faster than before, from a few days to as little as a few minutes. Moreover, new SURS provide the opportunity to take the data received and export it into electronic files for manipulation and investigation. Ultimately, the impact of these systems is like giving the investigator an extra month of time, time in which he or she can conduct more investigations. The end result is a SURS process that is dependent only upon how staff can adapt to this new technology and

incorporate the software into their daily work practices.

- Enhanced SURS also can yield:
  - A positive impact on employees vis-a-vis greater job satisfaction and higher morale;
  - Less staff turnover / higher staff retention rates;
  - Enhanced program credibility with providers, legislators, etc.;
  - Better opportunities for program evaluation research;
  - The ability to evaluate managed care encounter data; and
  - The ability to assess new programs or policy changes more expeditiously, in months rather than years.

Medical Transportation: *Electronic fraud detection technology and statistical analysis are being used successfully by the State of Illinois to detect fraudulent billings by medical transportation companies. This session explored the collaborative work of the Illinois Department of Public Aid (IDPA), the Federal Bureau of Investigation, and the U.S. Attorney's Office for the Northern District of Illinois in several fraud cases based in part on findings from the IDPA's payment error study and follow-up analysis of non-emergency transportation claims in Project NET. The panelists discussed the problem solving and follow-up approaches for developing additional evidence and how they cooperated to overcome potential obstacles that might have precluded them from making successful criminal and civil fraud cases.*

Speakers:
Wayne Oakes, Supervisory Special Agent, Federal Bureau of Investigation (moderator)
Robb Miller, Inspector General, State of Illinois
Amy St. Eve, Assistant U.S. Attorney, Northern District of Illinois

---

- The state Office of Inspector General (OIG) has a longstanding commitment to empirical research into fraud and abuse, and employs six staff researchers. The OIG maintains a close relationship with that state's Medicaid staff and MFCU, and there is a health care fraud task force in every district in the state.

- Ten transportation audits have been conducted at the request of law enforcement. The OIG found $4,443,263 in overpayments, and five transportation providers already have been terminated.

- The state conducted a Medicaid payment accuracy rate study in 1998, finding the area of nonemergency transportation to be one of the most critical concerns. The OIG examined a statistically valid random sample of 599 medical services of all sorts, finding an overall five percent payment accuracy rate. Though nonemergency transportation costs were not a substantial portion of the state Medicaid budget, percentage-wise, nonemergency transportation accounted for the largest category of payment error in the study, with 31 percent, or $11.55 million of $37.2 million spent, estimated to be in error.

- In the Medicaid context, nonemergency transportation is viewed as problematic for a number of reasons. It is one of the few reimbursable areas where individuals other than medical professionals can render service and perform their functions with almost complete autonomy. For most types of transportation providers, these individuals and the firms for which they work are not licensed by any state professional or health care licensing authority. It is frequently difficult to determine whether the provider or the client or both are responsible for the misspent funds. It is one of the few areas where clients can easily defraud the system. It is difficult, if not impossible, for the honest provider to be sure that the client is using the service to obtain legitimate medical care rather than other, non-medical reasons, such as shopping or employment.

- Using data provided by the OIG, the FBI launched "Operation Transport" looking at four nonemergency transportation providers. Audits revealed erroneous billing, aberrant billing patterns, and billing for inflated transport mileage.

- Project "NET" (nonemergency transportation), conducted by IDPA OIG was intended as a "quick response" project that reviewed claims paid to 64 nonemergency transportation providers that were among the highest reimbursed for calendar year 1998. The unit of analysis was services provided during the month of March 1999. Fifty claims per provider were reviewed, or if the provider submitted fewer than 50 for the month, then all claims that were submitted. Of 12,323 services reviewed, 6,068 discrepancies were noted, with some services having more than one discrepancy. Missing or inadequate records were found in 32.1 percent of services and accounted for 78.4 percent of the total discrepancies. A total of 17.2 percent of all discrepancies involved the billing of excess mileage. An attempt was made to verify that nonemergency medical transportation services matched to a Medicaid claim on the same date revealed that only 52.1 percent of nonemergency services could be matched to a Medicaid claim, with the rest questionable. Other findings included double billing, billing for services never rendered, and billing for unauthorized attendant services. The study estimated that the 64 providers examined were overpaid $24,810 for March 1999 dates of service, constituting 33percent of their payments for that month's services.

- From the study, the IDPA OIG developed a number of recommendations:
  - Include nonemergency transportation providers in a proposed random claim review process;
  - Require standard documentation forms;
  - Educate providers to better understand record keeping and retention requirements;
  - Evaluate accurate methods of calculating mileage;
  - Privatize the prior approval process; and
  - Provide training to state human services staff on prior approval requirements.

- One case in particular involved Frytag Ambulance Company, which originated as a referral from a contractor, and involved billing for services not medically necessary. The case was developed using the paramedical transport staff as key witnesses, using surveillance which yielded evidence of patients being walked to ambulances, and speaking with registered nurses staffing the dialysis centers to which patients were transported for treatment and later transported home. Criminal convictions on charges of defrauding Medicare and Medicaid were obtained on all counts charged, and statistical sampling was used in the sentencing process. In its defense, Frytag argued that the patients they transported were very sick, and that the Medicare regulations are not clear.

- Another case, handled as a civil matter, involved Ezra Transportation, which was accused of double billing and other abuses. Audit findings were used to seize assets, but after settlement, the company was reconstituted under a different name.

Complex Network Fraud Schemes: *How can health care claims data be examined across multiple levels and/or sources to reveal illicit networks of billing relationships among providers and other collaborators? This session profiled such work based on provider-beneficiary "ping-pong" and "link analysis" technology to identify potentially fraudulent pharmacy billings in California and fraud schemes by durable medical equipment suppliers, clinics, home health and assisted living facilities in Florida.*

Speakers:

Jean Bishop, PriceWaterhouseCoopers (moderator)

Barbara Bisno, Assistant US Attorney, Civil Division, Southern District of Florida, US Department of Justice

Dennis Cowan, Arthur Andersen Consulting

Sharon Houser, Auditor, US Attorney's Office, Middle District of Florida, US Deptartment of Justice

Rob Moser, International Business Machines

- This session discussed methods and approaches for identifying and investigating illicit networks of providers and beneficiaries. Data analysis to identify the linkages and associations between providers, and among providers and "shared" beneficiaries, serves as a starting point for further investigation. Networks between providers are often legitimate, so further research and investigation are essential to determine whether fraud or abuse may account for these associations. Several tools developed to identify such networks are available currently. The three speakers described several cases involving possible Medicaid fraud in California and Medicare fraud in Florida.

- For one state Medicaid program, pharmaceutical claims in a large metropolitan area were analyzed using "ping-pong" and "link analysis" technologies to identify a network of providers who collaborated to bill nearly $1.5 million of possibly fraudulent Medicaid claims. Geographic analysis of beneficiary residences and of the pharmacy locations was used to support the theory that Medicaid beneficiary numbers were used inappropriately to facilitate fraudulent billings. Subsequent investigation revealed that these pharmacies had virtually no records of transactions or documentation to support claims filed. One pharmacy owner was found to have been convicted previously for a health care fraud offense and was barred from participating in the Medicaid program. A criminal investigation is ongoing. A physician who wrote most of the prescriptions for this pharmacy also is under investigation.

- The Medicare Part B contractor in another state provides to the U.S. Attorney's Office (USAO) numerous routine reports based on analyses of claims data using a variety of analytical approaches and tools for ongoing investigations and top billing providers. Some of these reports examine beneficiary and provider links and/or networks, such as:
  - Address Clustering and Geographical Zip Codes - to ascertain if a certain geographical area is being targeted by providers for fraudulent scams; and
  - Beneficiary "Ping-Ponging" - to detect when a beneficiary or a beneficiary's health

insurance number is being passed from one provider to another, and to evaluate common ownership or recruiting sites.

- The USAO has prosecuted several cases that were facilitated by data analysis examining provider-beneficiary networks. Two were described during the presentation:
  - The first was a multi-million dollar scheme involving a durable medical equipment (DME) supplier associated with impotence clinics, clinical labs, a mobile diagnostic facility, and several doctors. Kickbacks for patient referrals were disguised through room rental leases and no-interest loans; also sums of $200-250 were paid for each patient referral between the impotence clinics and DME supplier. The principal defendant was convicted criminally and sentenced to prison and over $2 million was recovered.
  - The second case involved collusion between a DME supplier and distributor who targeted beneficiaries in a certain geographic area to generate claims for unnecessary DME purchases. Rapid escalation in this DME distributor's claims for wheelchairs and beds - $7 million in two years - was detected by the Medicare contractor. Subsequent data analysis identified associated providers and beneficiaries and facilitated the U.S. Attorney's office investigation. This case is still ongoing.

- Another USAO began applying technology to health care fraud in 1995 when the office obtained funds to hire a computer specialist and purchased a stand-alone computer with the capacity to handle large databases. The Office's first achievement was gaining approval from HCFA and the carriers to provide every other month a list of current Part B providers located in the district, with addresses, owners, Medicare amounts paid, and complaints registered. This immediately facilitated investigations and reduced the number of requests from AUSAs and agents for this type of basic information regarding providers who came to the Office's attention in investigations. The Office's second achievement was an agreement among all state and federal investigative agencies and the USAO to share the names of all targets of civil and criminal investigations, which is distributed on disk to all agencies and is updated by the USAO on a quarterly basis. Each agency checks this list of all investigations to determine if a potential target is already being looked at by another agency.

- At the beginning of an investigation, the office obtains data for the provider and beneficiary billing histories, which then is sorted by top referral sources and frequently used procedure codes. Depending on the type of provider, or other information known about the provider, other sorts can be done. The beneficiary histories also can be sorted by diagnosis code, providers, and other relevant issues. Analysis of claims data histories have led to discovery of illicit provider networks. For example, a ping-pong analysis of beneficiaries in a home health investigation revealed that a sister home health agency billed for the same beneficiaries as the original target agency, for the same diagnosis, and was referred by same doctors. This investigation led to freeze of $900,000 of fraudulent payments.

- Another case involved billings by a respiratory therapy services company that was discovered

as a result of bank suspicion of money laundering. Data analysis of beneficiaries, grouped by address and then sorted as groups by address, led to the discovery that this company preyed upon residents of assisted living facilities (ALFs). These ALF beneficiaries were too frail to receive respiratory therapy, which was easily shown by an expert witness. A ping-pong report revealed four related companies that were included as targets. A report on top physician referrers indicated three doctors were responsible for 90 percent of referrals. This ultimately led to admissions by doctors that they had not seen patients before making referrals and that they had kickback arrangements with ALF owners. This case led to a freeze of $1.8 million in suspected fraudulent payments.

Glossary of Terms Used in this Document

Address clustering - An approach to claims data analysis that ascertains whether a particular geographic area is being targeted by providers for fraudulent claims.

Beneficiary Integrity Support Center (BISC) - A geographically based HCFA Program Safeguard Contractor (PSC) that works closely with carriers and fiscal intermediaries to support data analysis capacity and provide specialized data analysis services focused on identifying fraud schemes.

Core Detail Information System (CDIS) - A national database maintained by TRICARE, the US military's health plan, the CDIS tracks utilization and stores more than 90 million claims. With its ability to identify abnormal billing patterns, CDIS offers a way to evaluate allegations and suspicions and reduces the need for audits.

Data mining - The process of extracting, from large pools of data or databases, information that can be examined for hidden patterns, trends, relationships and correlations among the data by using existing data analysis software. Data mining software is particularly useful when dealing with a large volume of data and complex interrelationships among providers, beneficiaries, and claims.

Data warehouse (or data mart) - A collection of integrated, subject-oriented databases with the ability to merge operational, informational, departmental and beneficiary data. A key feature of a data warehouse is that data from a transaction-driven operational system is replicated into a relational database designed for ready access to large amounts of data outside of the operational system, lending itself well to analytical processing over long, historical perspectives.

Decision support system (DSS) - A generic term describing a menu of hardware and software components that can be combined to facilitate access to data and its analysis for a wide range of end-users. A DSS allows these users to directly access and manipulate data from their desktops without having to send data or report generation requests to a data processing shop or fiscal agent for processing. Typical functions that are supported by a DSS include utilization management, provider/beneficiary/health plan profiling, and contractor performance evaluation.

Drill down - The ability to move from a more general level of detail to a finer level of detail.

Enrollment Database (EDB) - In general vernacular, a health plan database containing information about all individuals registered to receive benefits from a health care program (e.g., Medicare) including demographic information, enrollment dates, third party buy-in information, and/or managed care enrollment. In the Medicare context specifically, a database that serves as the authoritative source for beneficiary entitlement information. HCFA has developed a State extract from this database to support State Medicaid Agencies' needs for information about beneficiaries dually eligible for Medicare and Medicaid.

Fraud and abuse detection system (FADS) - A system that implements neural and learning technology for the detection of fraud and abuse in health and human services programs.

Fraud Investigations Database (FID) - A comprehensive, nationwide system devoted to Medicare and Medicaid fraud and abuse data and the information-sharing process among government agencies, the FBI, DOJ, State MFCUs, Postal Inspectors' offices, Medicare contractors, and other program integrity stakeholders. Among other information, the FID provides the status of all Medicare and Medicaid fraud cases being handled by HCFA, its contractors and law enforcement agencies.

Fraud score - An index of suspicion yielded by a predictive model, in which the system generates reasons for the user to drill down to the patient, claim, or procedure level to determine the rationale behind the fraud score.

Fuzzy Logic - A form of logic used in some expert systems and other artificial-intelligence applications that processes data by monitoring very subtle degrees of abnormality for any given behavior. This technology weights factors and measures them collectively to reach certain conclusions and is suitable for detecting potential fraud and abuse because it takes into account many different factors at once. For example, the number or percentage of patient visits to a provider on Sundays and holidays can be combined and weighted with other data, such as the number of duplicate bills submitted. This information is then scored and measured against a peer group score.

Link analysis technology - Data analysis technology that is used to identify linkages and associations among providers that may be attributable to fraud and abuse schemes such as "beneficiary sharing" rather than to legitimate provider networks.

Medicaid Management Information System - With a few exceptions, State Medicaid Agencies are required to maintain an MMIS, which is an automated claims payment and information retrieval system featuring quarterly tape extracts of individual eligibility and fee-for-service claims records from States' Medicaid claims processing systems. The primary reporting medium for Medicaid program statistics, MMIS provides the infrastructure for a person and claim-level national database, which can handle capitated encounter data.

Medicaid Fraud Control Unit (MFCU) - A single, identifiable entity of state government that is composed of at least one attorney, one auditor, and an investigator who are charged with investigating, and in many cases prosecuting, Medicaid fraud cases. A MFCU, which operates under a Memorandum of Understanding with the State Medicaid Agency and subject to oversight by the DHHS' OIG, frequently resides in the State's Attorney General's office.

Medicare Integrity Program - An initiative, authorized by provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law No. 104-191), which provided

HCFA with stable, increasing funding for Medicare payment safeguard activities. These provisions also granted HCFA new authority to contract with entities, in addition to Medicare carriers and fiscal intermediaries, to perform specific payment safeguard functions.

Minimum Data Set (MDS) - A collection of 24 quality indicators, the Minimum Data Set (MDS) is part of the federally mandated process for clinical assessment of all residents in Medicare or Medicaid certified nursing homes. This process provides a comprehensive assessment of each resident's functional capabilities and helps nursing home staff identify health problems. Resident Assessment Protocols (RAPs), are part of this process, and provide the foundation upon which a resident's individual care plan is formulated. MDS assessment forms are completed for all residents in certified nursing homes, regardless of source of payment for the individual resident. MDS assessments are required for residents on admission to the nursing facility and then periodically, within specific guidelines and time frames.

Network identification - A process that computes the measure of relationships between entities in the guise of a "dissimilarity index" and can be used retrospectively to review top-ranked networks to determine legitimacy *(i.e.,* to identify potential cases of fraud), set benchmarks for the future, and review and test for changes over time. Network identification can provide an early warning by identifying new networks and significant increases in rank, permitting real-time response including determining potential exposure, looking at past instances of abuse, and setting up program safeguards.

Neural network - Like data mining, a neural network utilizes high-speed, high-volume technologies that approach real-time analysis of claim and encounter data to look for unexpected and suspicious patterns at the time of the transaction. Although effective for early detection of newly emerging scams to facilitate the development of prepay controls, neural technology can be resource intensive in terms of both cost and expert staff support. (See also predictive model.)

OSCAR - HCFA's online survey, certification, and reporting system, which contains descriptive information about nursing home ownership, complaint and enforcement resolution, and previous survey results.

"Ping-Pong" scheme analysis - An approach to claims data analysis that detects when a beneficiary or a beneficiary's health insurance number is being passed among providers; also evaluates common ownership, referral practices, or recruiting sites.

Predictive model - The use of sophisticated, dynamic computing power to collect information including claims data, facility and provider information, licensing information, and patient demographics, and to organize the data so as to describe an entity's typical behavior and behavioral features. Unlike static fraud detection measures that can become ineffective, the predictive model looks globally to detect behavior indicative of potential fraud and abuse and is capable of continually evolving to detect new fraud schemes.

Program Safeguard Contractor (PSC) - An entity that, under contract with HCFA, performs program safeguard activities that were previously performed exclusively by Medicare carriers and fiscal intermediaries. Under authority provided in provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law No. 104-191), PSCs conduct medical review, cost report audit, and fraud detection and prevention functions as part of the Medicare Integrity Program.

Resource utilization group (RUG) - A classification system for nursing home residents, the RUG is a composite measure used to group residents with similar resource utilization and clinical characteristics. Resources include time spent on care, non-rehabilitation ancillaries, general services and capital expenses.

Service bureau model - An electronic fraud detection system installation model featuring offsite programming and data analysis, which minimizes costs and organizational training issues. The service bureau model may preclude the ability to rapidly run new or modified queries, and may entail security and confidentiality issues arising from the transmission of data to the offsite facility. (Contrast with the turnkey model.)

Statistical Analysis Contractor - A PSC that provides HCFA with comprehensive, ongoing analysis of trends, utilization data and other information to assist in the detection of fraudulent and abusive behavior.

Statistical outlier - An observation in a set of data that appears to be inconsistent with the remainder of that set of data.

Surveillance and Utilization Review Subsystem (SURS) - The primary purposes of a SURS, which is a subsystem of MMIS, is to process information on medical and health care services to assist Medicaid program managers and to identify providers and Medicaid beneficiaries who are most likely to defraud the Medicaid program. State SURS staff performs postpay utilization review of providers and beneficiaries to identify questionable patterns of services delivery and utilization. This review uses profiling systems that employ indices of fraud and abuse based on comparisons with normal service utilization.

Turnkey model - An electronic fraud detection system installation model in which users install the product on their own computer hardware. Because data is processed in-house rather than having to be transmitted to another entity for generating findings, the turnkey model may yield quicker results. Conversely, this approach may present relatively higher installation costs, issues of compatibility with present systems, and require additional specialized staffing or training. (Contrast with the service bureau model.)

Action Plan based on Working Group Recommendations

Conference participants were assigned to seven geographically based, facilitated working groups, each of which covered substantially the same issues. Participants were invited to discuss their most pressing needs related to high-tech tools for fraud and abuse detection, investigation and prosecution. They identified and ranked major obstacles to more effective use of technology in their program integrity efforts. They also brainstormed suggestions for follow-up action for HCFA and DOJ consideration and implementation.

Conference organizers from HCFA, including representatives from Medicare and Medicaid, and DOJ developed the following Action Plan from the recommendations of the working groups.

1. A National Technology Group (NTG) should be formed.

- The NTG would:
  - Address technology, fraud detection and data sharing issues, as well as policy, operations, resources and barriers related to using technology and data mining to combat health care fraud and abuse;
  - Serve as a clearinghouse for best practices in using technology for fraud and abuse detection and for vendor information;
  - Disseminate results of successful anti-fraud activities and coordinate training conferences; and
  - Initiate and coordinate with Regional Technology Users Groups (RTUGs).

- Composition would be limited to no more than 25 representatives of DOJ, HCFA (Medicare and Medicaid), the FBI, HHS/OIG, TRICARE/DCIS, OPM/OIG, the National Association of Medicaid Fraud Control Units, and State Medicaid Agencies. Both program integrity staff and technical/analytical staff should participate. The group should be chaired by HCFA's Program Integrity Group.

- A kick-off conference, attended by moderators, key agency representatives, and the regional working group facilitators from the 2000 national conference and targeted for spring or early summer 2001, would establish the group and set future priorities. Potential agenda topics include:
  - Information sharing and access to data;
  - Data analysis training;
  - Staffing, hardware and software resource issues;
  - Standardization needs;
  - Multi-level collaboration, communication and interaction;
  - Medicare and Medicaid data compatibility and consolidated analyses;
  - Availability of high-tech data analysis tools; and
  - Privacy limitations on data sharing.

- The NTG would establish and organize RTUGs by:
  - Designating initial chairpersons to organize and convene the first meetings;
  - Determining the manner of reporting back to the NTG
  - Discussing representation of RTUGs on the NTG; and
  - Establishing a timetable for developing Regional Users' Conferences.

2. Regional Technology Users Groups should be formed.

- Each RTUG would largely define its own purpose, with a "nuts and bolts" approach to issues and cases.

- RTUGs would be open to all program oversight and law enforcement organizations within the region and will work with existing Health Care Fraud Task Forces and Medicare Integrity Program contractors operating within their region.

- An initial chairperson for each RTUG would be designated at the NTG kick-off meeting. The RTUGs could be formed at Regional Users' Conferences or at RTUG kick-off meetings with interested parties initiated by the chairpersons.

- Meeting agendas would be set regionally by each RTUG, although agenda items could be offered by the NTG. The NTG will establish agenda items for the initial meeting of each RTUG.

3. HCFA should continue to expand fraud and abuse initiatives, including more conferences.

- Plan another national conference with a tentative target date of March 2002.

- HCFA and its contractors should expand their educational efforts, particularly by addressing a need for training on coding, policies, and data sources administered by HCFA.

- Focused instruction on data interpretation and analysis techniques, as well as attendant technology and systems issues, should be offered to U.S. Attorneys and other law enforcement agencies.

- Expanded educational efforts would be well served by incorporating "lessons learned" by State Medicaid Agencies.

- A secured Internet site administered by HCFA is a potential platform to support the need for enhanced information sharing.

4. Efforts to promote the use of technology to combat fraud and abuse should occur in

coordination with existing Federal-state-local health care fraud task forces.

- Conference participants concurred on the importance of reinforcing the multi-agency task force model as an effective means of sharing information and pooling resources.

SUMMARY RESPONSES TO QUESTIONS FOR WORKING SESSION DISCUSSIONS

1. **WHAT ARE THE MOST PRESSING "UNMET NEEDS" IN YOUR REGION (OR STATE) WITH REGARD TO TECHNOLOGY AND HIGH-TECH TOOLS FOR HEALTH CARE FRAUD & ABUSE (HCF&A) DETECTION, INVESTIGATION, AND PROSECUTION?**

Most Common "Unmet Needs"	***# of Regions***	***Regions Citing as an "Unmet Need"***
A) Information Sharing and/or Access to Data	10	All 10 Regions
B) Training for analyzing data; using technology and high-tech tools	8	Regions 1&2; 3B; 4; 5; 8, 9 & 10
C) Resources (staffing; hardware, software)	6	Regions 1 & 2; 3A; 8, 9 & 10
D) Lack of Standardization (e.g., to facilitate data sharing and cross-claims analysis)	6	Regions 4; 6 & 7; 8, 9 & 10
E) Collaboration, communication, and interaction among Federal & state health care program and law enforcement agencies	6	Regions 1 & 2; 5; 8, 9 & 10
F) Differences/incompatibility between Medicare and Medicaid data/information	5	Regions 1 & 2; 3A; 6 & 7
G) Lack of high-tech, data analysis tools	5	Regions 1 & 2; 4, 6 & 7
H) Speed up response time for fulfilling information requests	5	Regions 3B; 4; 8, 9 & 10
I) Joint database with access to HCFA data files and guide describing data files	3	Regions 3B; 4; 5
J) Help for States to develop fraud detection systems	3	Regions 1 & 2; 4
K) Privacy limitations against data sharing	3	Regions 1 & 2; 3A
Note: Numerous other "unmet needs were cited by one or two regions.		

2. **SEEK RESPONSES AND POSSIBLE SOLUTIONS TO THE FOLLOWING MAJOR OBSTACLES TO MAKING MORE EFFECTIVE USE OF CURRENT TECHNOLOGY AND HIGH-TECH TOOLS FOR COMBATING HCF&A IN YOUR REGION (STATE).**

Regions Confirming Obstacle (& Offering Solutions)

A. Lack of resources.	**All Regions.** Solutions: To obtain more money or funding (3B). Meet with carrier monthly, not after suspension; partnering with U.S. Attorneys and OIG instead of funnel down process (4). Participate in multi-agency task forces to allow agencies to pool resources (5).
B. Differing views of the results produced by the technology or high-tech tools (e.g., is it fraud, abuse, or error?).	**Regions: 1 & 2, 3A, 3B, 5, 6 & 7.** Solutions: Sharing of information between federal health care program and law enforcement agencies (3A). Need for the federal government to define what is "fraud" as distinguished from "abuse" (6&7).
C. Inability to take the "next steps" after data analysis.	**Regions: 3B, 6 & 7, 8, 9 & 10.** Solutions: Make sure you are on firm ground when you think you have identified fraud. Analyze policy statements (3B). Agencies and contractors need to develop consistent methods for evaluating and prioritizing work. The federal government should develop timelines and time limits for Medicare and Medicaid contractors to develop cases and for law enforcement agencies to take action (6&7).
D. Lack of information sharing or collaboration (e.g., program or contractor staff; investigators and prosecutors; states and federal government).	**Regions: 1 & 2, 3A, 3B, 5, 6 & 7, 8, 9 & 10.** Solutions: Involve prosecutors in the early stages of an investigation; keep the channels of communication open. Develop regional task forces that share concrete information about fraud patterns (3A).
E. "Medical records privacy" issues (e.g., concerns for violating patient-physician confidentiality through promoting data mining).	**Regions: 3A, 5, ,6 & 7, 8, 9 & 10.** Solutions: Need federal guidance regarding medical records privacy issues and information sharing between federal and state agencies and private insurers. Task forces should share concrete information about specific fraudulent patterns (3A).
F. Other Major Obstacles? (e.g., others mentioned by break out group participants)?	**Regions: 1 & 2, 3A, 5, 6 & 7** See Other Major Obstacles in response to Question 3.

3. AMONG THE OBSTACLES A-F IDENTIFIED IN QUESTION 2, PLEASE RANK THEM ACCORDING TO RELATIVE IMPORTANCE (E.G., MOST TO LEAST IMPORTANT).

	Overall Ranking of Importance	***Ranking of Importance by Each Regional Group***					
Obstacles Identified in Question 2	**1 & 2**	**3A**	**3B**	**4**	**5**	**6 & 7**	**8, 9&10**
A. Lack of Resources	4	1	1	2	2	1	1
B. Differing views of the results produced by technology (e.g., is it fraud, abuse, or error?)				4		4	
C. Inability to take the "next steps" after data analysis.						2	
D. Lack of information sharing or collaboration.	2	2	4		1	3	2
E. Medical Records Privacy issues		3	3		4	6	8
F. Other Major Obstacles? (suggestions of WG participants)							
(1) Need for change in 60-day rule	1a						
(2) Timely or readily available data in a standard format	3			1			3
(3) Streamline ADP process	5						
(4) Differences in program coverage (Medicare and Medicaid)		4					
(5) Lack of effective task forces among investigative agencies		5					4
(6) Lack of case coordination between law enforcement and contractors	1		2	3			7
(7) Move certain functions to Medicare Integrity Program (e.g., provider enrollment)				5			
(8) Need for data analysis					3		
(9) Amount of time needed to fulfill law enf. case development requests						5	
(10) How to access to national databases							5
(11) Assisting each other							6

4. **WHAT SPECIFIC "FOLLOW-UP" ACTIONS IN RESPONSE TO THIS CONFERENCE [AND/OR THE VARIOUS PLENARY, BREAKOUT, AND WORKING SESSION DISCUSSIONS] DO YOU RECOMMEND BE CONSIDERED BY HCFA AND DOJ FOR IMPLEMENTATION?**

Conference attendees were informed that representatives from each working group and HCFA and DOJ conference planning staff would prepare a "Proceedings of the Conference Report" to include recommendations offered by the regional working group participants that would be presented to the Executive Health Care Fraud Policy Group (comprised of the Deputy Attorney General, HCFA Deputy Administrator, HHS Inspector General). The following table summarizes the most common recommendations suggested by more than one working group.

Most Common Recommendations	***# of Regions***	***Specific Regions Making Rec.***
A) Form a National Technology Users Group	8	Regions 3A; 3B; 4; 6&7; 8, 9 &10
B) Form Regional Technology Users Groups	8	Regions: 1&2; 3A; 3B; 4; 8, 9&10
C) Strengthen or Enhance Task Forces of Law Enforcement and HCFA program personnel	7	Regions: 1&2; 3B; 4; 8, 9 & 10
D) HCFA should continue to expand fraud and abuse initiatives and use of national and/or regional conferences	6	Regions: 5; 6 & 7; 8, 9 & 10
E) HCFA should act as case coordination point and promote information sharing through a secure website (e.g., to catalog cases, fraud and abuse schemes, tools, analytical techniques, and to facilitate questions/dialogue	3	Regions: 5; 6 & 7
F) Improve data matching/sharing capabilities	3	Regions: 3B; 6 & 7
G) Medical records privacy issues (Note: The conference preceded the issuance of the medical records privacy rule in December 2000)	3	Regions: 1 & 2; 3A
H) Enhance Training (e.g., data analysis, use of high-tech tools, interpreting work products, etc.)	2	Regions: 3A; 3B