Testimony before the United States Senate
Committee on Homeland Security & Governmental Affairs,
Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security

Harnessing Technology and Innovation to Cut Waste and Curb Fraud in Federal Health Programs
Testimony of Lewis Morris
Chief Counsel
Office of Inspector General
U.S, Department of Health and Human Services

July 12, 2011
2:30 P.M.

Room SD-342, Dirksen Senate Office Building

Testimony of:
Lewis Morris
Chief Counsel
Office of Inspector General
U.S. Department of Health & Human Services

Good afternoon, Chairman Carper, Ranking Member Brown, and other distinguished Members of the Subcommittee. I am Lewis Morris, Chief Counsel to the Inspector General of the U.S. Department of Health & Human Services (HHS or the Department). Thank you for the opportunity to testify about the role new technologies can play in cutting waste and fraud in the Federal health care programs.

Program integrity efforts are enhanced by new information technologies and benefit from collaboration with the private sector, especially health insurers with whom we share investigative techniques and intelligence. My testimony provides several examples of how advanced data analytics are helping us conduct risk assessments, more effectively pinpoint our oversight efforts, and significantly reduce the time and resources required for audits, investigations, and other program integrity activities.

However, technology is not a silver bullet, and now more than ever, experienced professionals are integral to protecting Medicare and Medicaid. It is also important to be mindful that as program integrity efforts become more technology driven, so will health care fraud and we must adapt to this evolving environment. Additionally even the best fraud prevention technologies will be of little value if not effectively implemented and appropriately overseen.

New Technologies Hold Tremendous Potential for Enhancing Our Fraud Fighting Efforts

OIG is using information technologies and analytics, including data mining, trend evaluation, and modeling, to better identify fraud vulnerabilities and target our oversight efforts. OIG is leveraging an analytical foundation that provides an enterprise view of questionable activities, suspected fraud trends, and prevention opportunities. When united with the expertise of our agents, auditors, and program evaluators, OIG brings a formidable combination of cutting edge techniques and traditional investigative skills to the fight against fraud, waste, and abuse.

OIG's data warehouse is a key component of our strategic use of information technologies. Among other things, the warehouse integrates data from Medicare Parts A, B, and D so we can develop a more comprehensive picture of beneficiaries' histories of medical care and providers' billing patterns. For example, we can flag Part D prescription drug claims where there is not a related physician or hospital claim under Parts A or B, the absence of which suggests possible fraud.

In addition to adding powerful analytic tools, the data warehouse has the potential for dramatically improving the timeliness and impact of our work. Prior to developing the warehouse, OIG analysts and auditors often waited months to access a data extract from

Medicare's National Claims History. Further delays resulted from writing and running the many mainframe-based applications needed to complete an analysis or data match. Having the claims data in-house also means that we no longer compete for time on the CMS mainframe servers and can introduce new data mining tools and other related databases tailored to OIG's oversight and enforcement work. Data matches that used to take weeks or months to complete are now performed in-house in a matter of hours.

Information technology enables OIG to expand our analysis of questionable billing patterns. For example, through data mining and analytics we found that Medicare was spending about $4,400 for inhalation drugs per beneficiary in south Florida compared to $815 per beneficiary in the rest of the country. Combining data from the manufacturer and wholesalers of a particularly expensive inhalation drug, we found that south Florida suppliers billed Medicare for 17 times more than the total amount of that drug sold to those providers. We can also more efficiently identify fraudulent claims for services provided to deceased beneficiaries, bills submitted by deceased providers, and health care providers who are using beneficiary numbers we know have been compromised.

OIG's Use of Information Technology To Support Audits

OIG's new hospital compliance initiative illustrates the impact of technology on our ability to identify suspect claims and non-compliant billing practices. Payments for inpatient and outpatient hospital services account for roughly 30 percent of the $515 billion spent on Medicare. Given these significant program outlays, OIG has deployed resources toward testing and ensuring the 3,600 acute care hospitals' compliance with program requirements.

In the past, OIG's hospital audits typically focused on a specific area of risk (e.g., unbundling of services, inpatient same-day discharges and readmissions, and credits for medical devices), and we audited claims exclusively related to that issue. In part, we had narrowly focused our audits due to limits on our capacity to store and match data. As a consequence of increased data storage, computer matching, and data analytic capabilities, we are now more quickly and efficiently analyzing a vast array of hospital data to simultaneously identify multiple compliance risks.

As part of our ongoing hospital audit initiative, we test hospitals against 27 risk areas that our prior audit and enforcement experience indicate are error-prone. To better focus our testing, we also analyze other hospital information, such as provider overpayment, Medicare exclusions, and law enforcement databases. Collectively, these data provide a comprehensive picture of how a hospital is performing and where compliance problems may exist. Using computer matching and data mining techniques, we then identify potential problem areas, select claims for testing, and conduct hospital site visits to perform comprehensive reviews of billing and medical record documentation. Hospitals must return any identified overpayments and are expected to implement necessary internal controls to prevent future improper billing. We have completed several such audits and have 40 more planned or underway. Two years ago, the data analytics would have taken weeks or months to execute. Now, it takes approximately 20 minutes to run the computer program for each hospital.

It is important to note that while the use of data analytics allows for a more efficient and targeted audit process, the expertise and insight of auditors, coding professionals, and medical consultants remain an essential part of this and any technology-assisted review. Medicine and the health care system are extremely complex. A data run, even if derived from sophisticated metrics and powerful computers, cannot replace the role of professionals who bring experience and insight to the analysis of that data. In short, technology can be a powerful tool in the fight against waste, fraud, and abuse, but it is not a stand-alone solution.

Given the magnitude of hospital expenditures, we believe this innovative use of information technology is essential to identifying and recovering improper Medicare payments. We plan to integrate this Part A hospital data with Parts B and D data to better understand relationships between provider groups and identify payment vulnerabilities in other areas of the Medicare Program. We will partner with CMS and hospitals as this initiative moves forward.

In addition to dramatically increasing the efficiency of our audits, this data-driven approach yields additional benefits. Adopting these types of data analytics, hospitals should be able to identify and correct compliance problems early before claim submission. We also have received feedback from the hospital community that these targeted audits enabled them to strengthen their compliance programs and address compliance more comprehensively instead of focusing on only singular issues.

OIG Use of Information Technology in Support of Fraud Investigations

As exemplified by the Medicare Fraud Strike Forces, sophisticated data analysis, combined with field intelligence and traditional law enforcement techniques, have enabled us to more quickly identify fraud schemes and trends. The data-driven approach of the Strike Forces pinpoints fraud hot spots through the identification of suspicious billing patterns and targets criminal behavior as it occurs. The Strike Force model has proven highly successful and has accelerated the Government's response to criminal fraud, decreasing by roughly half the average time from an investigation's start to the case's prosecution. Since their inception in 2007, Strike Force teams have charged over 1,000 individuals with seeking to defraud Medicare of more than $2.4 billion.

Advanced data analytics are enhancing not only our Strike Force cases but also our traditional investigative work. For example, in the recent investigation of Clinical Home Care, innovative data analysis, coupled with inter-departmental information sharing and agent field work, identified over $1.1 million in fraudulent claims. The efforts of OIG Special Agents, working in conjunction with other law enforcement partners and CMS's program integrity contractors, led to the arrest of those responsible for the submission of the fraudulent claims.

Relying on State corporation records and field intelligence, OIG identified a suspicious change in ownership of Clinical Home Care, a durable medical equipment company (DME) in Palm Beach, Florida. Using recently available data sources, including CMS's Next Generation Desktop database, OIG agents compared records of Medicare beneficiaries with compromised identification numbers with known fraudulent DME suppliers associated with Clinical Home Care and then identified thousands of suspect claims. OIG agents worked quickly with CMS's

Zone Program Integrity Contractor (ZPIC) to ensure that Medicare did not pay these claims pending the investigation. OIG arrested its first subject in this case only 30 days after the first fraudulent claim was submitted to Medicare. That subject, along with another individual, has since pled guilty. Thanks to a combination of technology, interagency collaboration and hard work, not a single dollar was lost due to these fraudulent claims.

While successful conclusion of a health care fraud investigation in 30 days is not the norm, this case exemplifies the exceptional results we can achieve by using technology, combined with agents' instincts and knowledge of evolving health care fraud schemes, interagency collaboration, and tips from citizens, in the investigation and prosecution of health care fraud.

Use of Information Technology To Strengthen Program Integrity

OIG's use of technology in support of its mission extends far beyond its audit, evaluative, and investigative work. We also will be using information technologies to better utilize one of the most powerful tools in our arsenal against fraud, abuse, and substandard care: the exclusion of individuals and entities from participating in Federal health care programs. Medicare and other Federal health care programs will not pay for services or products provided by excluded individuals or entities. If excluded from these programs, a dishonest health care provider is effectively out of business.

To notify health care programs and providers and prevent inappropriate payments to excluded parties, OIG posts its List of Excluded Individuals and Entities (LEIE) on the OIG Web site.[1] The list is updated monthly and is available in both on-line searchable and downloadable formats. To ensure that health care programs and patients are protected from all fraudulent, abusive, incompetent, or otherwise unfit providers, we work with our external partners in State Governments and other Federal agencies to receive referrals of individuals and entities that meet the criteria for exclusion.

To ensure the continued success of OIG's exclusion program in the 21st century, OIG is revamping our processes with a two-pronged approach: (1) improving coordination: we will improve the completeness of the LEIE by making it easier for external stakeholders to provide exclusion-related information to OIG, and (2) increasing communication: we will improve the accessibility of the database to health care providers and other users. In our efforts to meet both of these goals, we are examining new methods to deploy information systems and information technology that will promote better integration between existing OIG resources and those of our external stakeholders. The result of this effort will be a system that capitalizes on coordination and communication to effectively protect the programs and beneficiaries from untrustworthy providers of health care.

Increasing the streams of referrals from our external partners is also vital to our exclusion program improvement efforts. For instance, we receive important information from State licensing boards' notices of adverse actions that allows us to identify numerous individuals who

[1] http://www.oig.hhs.gov/exclusions/index.asp.

are subject to exclusion. However, we do not receive reports of all adverse actions from all States. State licensing boards are not statutorily required to refer adverse actions against providers to OIG. We currently receive this information on a voluntary basis from the State boards, general public notices of board actions in various States, or connections developed by OIG exclusions analysts. Furthermore, the manner and timing of the notices is entirely dependent on each State licensing board.

A legislative requirement for State licensure boards to provide notice of adverse actions to OIG would increase our ability to identify individuals subject to exclusion. Further, regular and standardized reporting of adverse actions from State licensing boards would allow for more timely identification of individuals subject to exclusion and could help prevent providers with significant adverse actions against their licenses from moving from State to State to continue providing care.

Sharing Intelligence With Private Health Care Insurers

OIG recognizes that private health care insurers have developed a tremendous wealth of experience and technological expertise in addressing our common goal of stopping health care fraud. It is axiomatic that most of the criminals who prey on the Nation's health care system are equal opportunity thieves – they defraud private health care insurance as well as the Federal health care programs.

Recognizing this fundamental principle, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) established and funds a program to combat fraud and abuse committed against all health plans, both public and private. This legislation required the Attorney General and the Secretary of Health & Human Services to establish a Health Care Fraud and Abuse Control (HCFAC) Program under the joint direction of the Attorney General and the Secretary (acting through the Inspector General). In furtherance of the goals of the HCFAC program, the Attorney General and Secretary issued a Program Statement and detailed set of Guidelines for joint HHS/Department of Justice (DOJ) activities to fulfill the dictates of HIPAA. One of the core concepts of the Statement and Guidelines is that "DOJ, HHS and other enforcement and program agencies will work together with the private sector to pursue a comprehensive enforcement approach to health care fraud. The foundation of this approach is coordinating and exchanging information in a regularized manner."

In furtherance of that core concept, the Program Statement and Guidelines outlines a rich menu of possible health care anti-fraud, program integrity, and information sharing activities between the Federal Government and the private sector. Among the contemplated activities are: 1) the establishment of working groups to examine particular areas of the health care industry in order to develop recommendations on enforcement policy; 2) the creation of mechanisms for government to alert the public, service providers, and consumers to fraud schemes; and 3) the development of mechanisms for identifying information concerning payment or record keeping policies, structures, or practices that make public or private health plans vulnerable to fraud, with OIG to compile and transmit reports on such vulnerabilities to the health plans so corrective action can be taken.

Since the creation of the HCFAC program, OIG, DOJ, and other law enforcement and program agencies have worked to carry out the objectives of the program. As part of that effort, United States Attorneys' Offices established Health Care Fraud Working Groups, which brought together government agencies and private sector insurers united in the common goal of combating health care fraud. These work groups have proven highly effective in promoting collaboration. Our agents report receiving significant field intelligence on ongoing fraud schemes and many have engaged in joint public/private investigations in which their private sector counterparts provided active assistance or staffing for the case.

Among the private sector organizations participating in this effort is the National Health Care Anti-Fraud Association (NHCAA). NHCAA is a national organization focused exclusively on the fight against health care fraud, whose members represent more than 100 private health insurers. Its mission is to protect and serve the public interest by increasing awareness and improving the detection, investigation, civil and criminal prosecution, and prevention of health care fraud. OIG takes an active role in training conferences and conducts regular liaison meetings with NHCAA in order to share information about significant areas of health care fraud exposure and emerging trends. In addition, an OIG investigator sits on the NHCAA board as the law enforcement liaison.

Efforts currently are underway to further enhance collaboration with the private sector. For example, the recent Health Care Fraud Prevention and Enforcement Team (HEAT) fraud summit in Philadelphia emphasized the critical importance of public-private collaboration in the fight against health care fraud.[2] Because useful information sharing often occurs between investigators at a case level, we are working with our law enforcement partners to provide "best practices" guidelines that can promote appropriate information sharing with the private sector.

Anticipating Vulnerabilities and Challenges Presented by the Use of Information Technology

As the Committee continues to explore ways in which new technology and private sector business practices can enhance program integrity efforts, it is important to be mindful of the ways in which fraud will evolve in response to new technologies, as well as the vulnerabilities associated with the electronic environment. It is also important to note some of the distinguishing characteristics of the Federal health care programs vis-à-vis private industry.

As program integrity efforts become more technology driven, so will fraud

For example, electronic health records (EHR) may not only facilitate more accurate billing and increased quality of care, but also fraudulent billing. The very aspects of EHRs that make a physician's job easier—cut-and-paste features and templates—can also be used to fabricate information that results in improper payments and leaves inaccurate, and therefore potentially dangerous, information in the patient record. And because the evidence of such improper behavior may be in entirely electronic form, law enforcement will have to develop new

[2] http://www.stopmedicarefraud.gov/.

investigation techniques to supplement the traditional methods used to examine the authenticity and accuracy of paper records.

Compounding this concern, OIG reports have identified significant vulnerabilities relating to the security of electronic patient health information. This work reveals inadequate protection of patients' health data at hospitals throughout the country and that existing Federal standards and certification criteria fail to address important information technology (IT) security controls. [3] These reports found, among other things, that many hospitals had inadequately safeguarded their wireless networks, leaving sensitive health information vulnerable to hacking. In addition, the Department has not promulgated policies that would help ensure that adequate general IT controls exist to protect networks and computer systems that contain EHRs. We recommended that the Department conduct compliance reviews to ensure that Security Rule controls are in place and operating as intended to protect personal health information.

The concerns about data security extend far beyond EHRs, and apply equally to our efforts to enhance program integrity through predictive analytics, integrated data repositories, and other new technologies. As we do so, we must be mindful that in an increasingly electronic environment, the ability for data to be compromised and subsequently used for fraud, waste, and abuse can quickly and quietly materialize.

For example, CMS and State government data centers process hundreds of terabytes of data each month. To put this in perspective, a terabyte is equal to 220 million pages of text. This vast amount of data is transmitted with varying degrees of control and oversight. Trends show that health care data, including beneficiary and provider information, is stolen and sold by organized crime rings or individuals. Provider and/or beneficiary information is being compromised by social engineering schemes such as phishing emails. Data breaches of public and private entities have been occurring worldwide at an alarming rate. And the attacks are becoming increasingly sophisticated and stealthy. In its August 2010 report, the Privacy Rights Clearinghouse estimated that since 2005, over 533.4 million records have been compromised in thousands of publicly disclosed breaches. The incidents involved breached consumer information, such as personal medical records, credit card numbers, and Social Security numbers.

Detecting health care fraud is more complex than detecting credit card fraud

While predictive analytics and other techniques have proven effective in identifying potential fraud in credit card transactions, there are distinguishing characteristics of the Federal health care programs that should be kept in mind. For example, CMS has launched a new predictive modeling tool that will eventually allow for improved fraud screening before claims are paid. OIG will be able to utilize the data derived from the predictive modeling to identify emerging

[3] *Nationwide Rollup Review of the Centers for Medicare & Medicaid Services Health Insurance Portability and Accountability Act of 1996 Oversight*; *Audit of Information Technology Security Included in Health Information Technology Standards*, available at http://oig.hhs.gov/newsroom/news-releases/2011/security.asp.

fraud trends. But there are key differences between the use of data analytic tools in the health care environment and the use of these tools by credit card companies.

Credit card transactions are typically submitted immediately at the place and time of service, so not only can the data be monitored in real time, but the transaction hits the credit card company's database in real time. One challenge in importing the retail industry's data analytics into the health care environment is that a health care provider can bill for a service months after the date of service. Further complicating matters, the claim for a service may initially meet all the conditions for payment but subsequently be revealed as improper. For example, an outpatient laboratory test may appear payable when initially submitted by the hospital. But under Medicare rules, separate payments for nonphysician outpatient services rendered within 72 hours of the day of an inpatient admission are not permitted. When the hospital later submits a claim for an inpatient stay that began within that 72-hour window, the claim for that laboratory test is improper. This is a very different scenario from a credit card company stopping someone who attempts to buy a jet ski in Galveston with a credit card issued to a long-time resident of New York City.

Moreover, the health care payor must assess not only whether an item or service was provided as claimed, but also determine whether it is medically necessary. The determination of medical necessity often requires information that is not apparent on the face of the claim. For example, in our recently released report on power wheel chairs, we found that sixty percent of power wheel chairs provided to Medicare beneficiaries in the first half of 2007 were medically unnecessary or had claims that lacked sufficient documentation to determine medical necessity.[4] Medicare paid $95 million for these claims, which on their face appeared legitimate. In short, health care is very complex and it is difficult to predict and prevent health care fraud relying solely on data analytics.

Notwithstanding some inherent limitations in applying credit card technologies to health care fraud, our law enforcement efforts are enhanced by new data analysis techniques. The results of the health care fraud Strike Forces demonstrate conclusively that data analytics can be successfully used to identify geographic fraud hot spots and program areas vulnerable to fraud, waste, and abuse. We are continuing to explore how best to expand the use of information technologies to other areas of health care fraud detection.

Effective Contractor Oversight is Critical to the Successful Implementation of Program Integrity Efforts

Although new information technologies hold promise for enhancing program integrity efforts, even the best fraud prevention techniques will be of no value if not effectively implemented and appropriately overseen. OIG work spanning over a decade has revealed persistent problems with the performance of CMS's program integrity contractors and ongoing vulnerabilities in CMS's oversight.

[4] *Most Power Wheelchairs in the Medicare Program Did Not Meet Medical Necessity Guidelines*, available at http://oig.hhs.gov/oei/reports/oei-04-09-00260.asp.

These concerns are relevant across the spectrum of program integrity contractors we have reviewed, dating back to our 1998 findings of inconsistent performance among the Fiscal Intermediaries' fraud units that preceded Program Safeguard Contractors (PSC) and Zone Program Integrity Contractors.[5] Almost a decade later, in 2007, we found that PSCs also performed inconsistently, varying substantially in the number of new investigations initiated and cases referred to law enforcement, and producing minimal results in key areas such as proactive data analysis.[6] In a separate review, we found that CMS oversight of PSCs was lacking: evaluations of PSCs' performance did not include sufficient information and were not completed in time for evaluation results to be used in determining whether PSCs' contracts should be renewed.[7] More recently, a 2010 review of overpayments referred by PSCs found that just 2 of the 18 PSCs were responsible for 62 percent of the total amount of overpayments referred to claims processors for collection.[8] In the same 2010 review, we found that millions in overpayments identified by the PSCs [9]

We have identified similar problems with the performance and oversight of Medicare Drug Integrity Contractors (MEDIC) and Recovery Audit Contractors (RAC). We found that MEDICs experienced significant problems accessing and using data, which hindered their ability to identify and investigate potential fraud and abuse using proactive methods such as data analysis. Furthermore, CMS failed to give MEDICs the necessary approval to conduct audits of Part D plan sponsors' compliance plans, an important oversight function.[10] In our 2010 assessment of the RACs, we found that over the 3 years of the demonstration program, they made only two fraud referrals and received no formal training from CMS regarding identification and referral of potential fraud.[11] Over the next year, we will issue additional reports on vulnerabilities related to ZPICs and MEDICs. As CMS moves forward with new efforts that rely on contractors to perform data-driven program integrity functions, it is important to be mindful of the need for meaningful performance evaluation and adequate oversight.

Conclusion

New technologies, advanced data analytics, and collaboration with the private sector are extremely valuable in the ongoing efforts to curb fraud and abuse in the Medicare and Medicaid programs. Although these developments are encouraging, we must be mindful that the growth of

---

[5] *Fiscal Intermediary Fraud Units*, available at http://oig.hhs.gov/oei/reports/oei-03-97-00350.pdf.
[6] *Medicare's Program Safeguard Contractors: Activities to Detect and Deter Fraud and Abuse*, available at http://oig.hhs.gov/oei/reports/oei-03-06-00010.pdf.
[7] *Medicare's Program Safeguard Contractors: Performance Evaluation Reports*, available at http://oig.hhs.gov/oei/reports/oei-03-04-00050.pdf.
[8] *Medicare Overpayments Identified by Program Safeguard Contractors*, available at http://oig.hhs.gov/oei/reports/oei-03-08-00031.pdf.
[9] *Collection Status of Medicare Overpayments Identified by Program Safeguard Contractors*, available at http://oig.hhs.gov/oei/reports/oei-03-08-00030.pdf.
[10] *Medicare Drug Integrity Contractors' Identification of Potential Part D Fraud and Abuse*, available at http://oig.hhs.gov/oei/reports/oei-03-08-00420.pdf.
[11] *Recovery Audit Contractors' Fraud Referrals*, available at http://oig.hhs.gov/oei/reports/oei-03-09-00130.pdf.

information technologies and the increased access to sensitive data will be accompanied by new and evolving fraud risks. The challenge for OIG is to continue to ensure appropriate implementation and provide vigorous oversight of these new technologies.

Thank you for the opportunity to testify.