# EXAMINING OPTIONS TO COMBAT HEALTHCARE WASTE, FRAUD, AND ABUSE

## HEARING

BEFORE THE

SUBCOMMITTEE ON HEALTH

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

NOVEMBER 28, 2012

**Serial No. 112–182**

Printed for the use of the Committee on Energy and Commerce

*energycommerce.house.gov*

U.S. GOVERNMENT PRINTING OFFICE
85–722 PDF WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

## COMMITTEE ON ENERGY AND COMMERCE

FRED UPTON, Michigan
*Chairman*

JOE BARTON, Texas
*Chairman Emeritus*
CLIFF STEARNS, Florida
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
*Vice Chairman*
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
BRIAN P. BILBRAY, California
CHARLES F. BASS, New Hampshire
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
ROBERT E. LATTA, Ohio
CATHY McMORRIS RODGERS, Washington
GREGG HARPER, Mississippi
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
PETE OLSON, Texas
DAVID B. McKINLEY, West Virginia
CORY GARDNER, Colorado
MIKE POMPEO, Kansas
ADAM KINZINGER, Illinois
H. MORGAN GRIFFITH, Virginia

HENRY A. WAXMAN, California
*Ranking Member*
JOHN D. DINGELL, Michigan
*Chairman Emeritus*
EDWARD J. MARKEY, Massachusetts
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DeGETTE, Colorado
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANICE D. SCHAKOWSKY, Illinois
CHARLES A. GONZALEZ, Texas
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland

## SUBCOMMITTEE ON HEALTH

JOSEPH R. PITTS, Pennsylvania
*Chairman*

MICHAEL C. BURGESS, Texas
*Vice Chairman*
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
TIM MURPHY, Pennsylvania
MARSHA BLACKBURN, Tennessee
PHIL GINGREY, Georgia
ROBERT E. LATTA, Ohio
CATHY McMORRIS RODGERS, Washington
LEONARD LANCE, New Jersey
BILL CASSIDY, Louisiana
BRETT GUTHRIE, Kentucky
JOE BARTON, Texas
FRED UPTON, Michigan *(ex officio)*

FRANK PALLONE, Jr., New Jersey
*Ranking Member*
JOHN D. DINGELL, Michigan
EDOLPHUS TOWNS, New York
ELIOT L. ENGEL, New York
LOIS CAPPS, California
JANICE D. SCHAKOWSKY, Illinois
CHARLES A. GONZALEZ, Texas
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
HENRY A. WAXMAN, California *(ex officio)*

# CONTENTS

WITNESSES

SUBMITTED MATERIAL

# EXAMINING OPTIONS TO COMBAT HEALTHCARE WASTE, FRAUD, AND ABUSE

**WEDNESDAY, NOVEMBER 28, 2012**

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON HEALTH,
COMMITTEE ON ENERGY AND COMMERCE,
*Washington, DC.*

The subcommittee met, pursuant to call, at 10:03 a.m., in room 2123, Rayburn House Office Building, Hon. Joseph R. Pitts (chairman of the subcommittee) presiding.

Members present: Representatives Pitts, Burgess, Shimkus, Blackburn, Gingrey, Latta, Lance, Cassidy, Barton, Pallone, Engel, Schakowsky, and Waxman (ex officio).

Also present: Representatives McKinley and Christensen.

Staff present: Matt Bravo, Professional Staff Member; Paul Edattel, Professional Staff Member, Health; Julie Goon, Health Policy Advisor; Sean Hayes, Counsel, Oversight and Investigations; Robert Horne, Professional Staff Member, Health; Ryan Long, Chief Counsel, Health; Carly McWilliams, Legislative Clerk; John O'Shea, Policy Advisor, Health; Monica Popp, Professional Staff Member, Health; Chris Sarley, Policy Coordinator, Environment and Economy; Heidi Stirrup, Health Policy Coordinator; Alli Corr, Democratic Policy Analyst; Amy Hall, Democratic Senior Professional Staff Member; Elizabeth Letter, Democratic Assistant Press Secretary; and Karen Nelson, Democratic Deputy Committee Staff Director for Health.

Mr. PITTS. The subcommittee will come to order.

The Chair recognizes himself for 5 minutes for an opening statement.

## OPENING STATEMENT OF HON. JOSEPH R. PITTS, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF PENNSYLVANIA

In May of this year, the Department of Justice brought charges against 107 individuals who bilked Medicare for over $452 million. Just seven individuals in Louisiana were responsible for over $225 million of this fraud.

In a separate case in February, a single Dallas doctor was arrested for making $350 million in false claims. In February of 2011, 114 individuals who had bilked over $240 million were arrested in another crackdown.

All told, that billion dollars in improper payments represents less than 2 percent of the estimated $60 billion annually lost to waste, fraud, and abuse.

As bad as that number is on its own, I want to put it into context. The Medicare program is running out of money. The CMS actuary predicts the program could be insolvent in just 5 years. As the Congressional Research Service wrote in a June 2011 report, quote, "As long as the Medicare trust fund has a balance, the Treasury Department is authorized to make payments on behalf of seniors."

However, the report continues, quote, "There are no provisions in the Social Security Act that govern what would happen if insolvency were to occur," end quote. The report contends that when insolvency of the Medicare program happens, quote, "There would be insufficient funds to pay for all Part A reimbursements to providers," end quote.

If Congress and the President support the idea that seniors should depend on the Medicare program to pay their provider bills, reform of the program through legislative action will be needed. The Medicare trustees in their 2011 report to Congress have already stated as much. One area of reform that I hope we can tackle in a bipartisan way is the area of fraud and abuse in the Medicare program.

The Federal Government has made strides recently to improve catching fraudulent providers and beneficiaries, and I commend them for their efforts. However, at the same time, they have largely failed to implement mechanisms that would prevent fraudulent payments from being made in the first place. Prosecuting offenders does not get all the money that they stole.

One such area is predictive analytics. CMS implemented the fraud prevention system in July of 2011 to analyze Medicare claims data using models of fraudulent behavior after such a system was shown to work well in the private industry. However, while the current system can draw on a host of data sources in support of its efforts, the system has not yet been integrated with the agency's payment processing system to allow for the prevention of payments until suspicious claims can be determined to be fraudulent.

Further, a recent GAO report stated that CMS has failed to define an approach for even measuring whether the current system is helping to prevent fraudulent billing. It is my firm belief that greater transparency from CMS with regard to current fraud programs is needed if we hope to build upon what is currently being done to make the program more secure.

Our Nation's seniors are counting on us to ensure that Medicare fulfills its promises. We can do that in part by making sure their premium dollars are managed wisely and not lost to con artists.

Our hearing today will discuss the efforts Medicare has undertaken currently to prevent fraud in government programs. In addition, the panel has generously offered us their time and expertise to explore emerging technologies and mechanisms that might help improve those efforts.

I want to thank all of our witnesses for sharing their thoughts with us today. And I am confident that these ideas can help generate a bipartisan effort to improve the solvency of the Medicare program in the coming Congress.

The Chair now recognize the ranking member of the Subcommittee on Health, Mr. Pallone, for 5 minutes.

[The prepared statement of Mr. Pitts follows:]

**Rep. Joseph R. Pitts**
**Opening Statement**
**Energy and Commerce Subcommittee on Health**
**Hearing on "Examining Options to Combat Health Care Waste, Fraud and Abuse"**
**November 28, 2012**

In May of this year, the Department of Justice brought charges against 107 individuals who bilked Medicare for over $452 million. Just seven individuals in Louisiana were responsible for over $225 million of this fraud. In a separate case in February, a single Dallas doctor was arrested for making $350 million in false claims. In February 2011, 114 individuals who had bilked over $240 million were arrested in another crackdown.

All told, that billion dollars in improper payments represents less than 2 percent of the estimated $60 billion annually lost to waste fraud and abuse.

As bad as that number is on its own, I want to put it into context.

The Medicare program is running out of money – the CMS Actuary predicts the program could be insolvent in just five years. As the Congressional Research Service wrote in a June 2011 report, "as long as the (Medicare) trust fund has a balance, the Treasury Department is authorized to make payments" on behalf of seniors.

However, the report continues, "there are no provisions in the Social Security Act that govern what would happen if [insolvency] were to occur." The report contends that when insolvency of the Medicare program happens, "...there would be insufficient funds to pay for all Part A reimbursements to providers."

If Congress and the President support the idea that seniors should depend on the Medicare program to pay their provider bills, reform of the program through legislative action will be needed. The Medicare Trustees, in their 2011 report to Congress, have already stated as much.

One area of reform that I hope we can tackle in a bipartisan way is the area of fraud and abuse in the Medicare program. The federal government has made strides recently to improve catching fraudulent providers and beneficiaries and I commend them for their efforts. However, at the same time, they have largely failed to implement mechanisms that would prevent fraudulent payments from being made in the first place. Prosecuting offenders does not get back all the money they stole.

One such area is predictive analytics. CMS implemented the Fraud Prevention System in July 2011 to analyze Medicare claims data using models of fraudulent behavior after such a system was shown to work well in the private industry. However, while the current system can draw on a host of data sources in support of its efforts, the system has not yet been integrated with the agency's payment-processing system to allow for the prevention of payments until suspicious claims can be determined to be fraudulent.

Further, a recent GAO report stated that CMS has failed to define an approach for even measuring whether the current system is helping to prevent fraudulent billing. It is my firm belief that greater transparency from CMS with regards to current fraud programs is needed if we hope to build upon what is currently being done to make the program more secure.

Our nation's seniors are counting on us to ensure that Medicare fulfills its promises. We can do that in part by making sure their premium dollars are managed wisely and not lost to con artists.

Our hearing today will discuss the efforts Medicare has currently undertaken to prevent fraud in government programs. In addition, the panel has generously offered us their time and expertise to explore emerging technologies and mechanisms that might help improve those efforts.

I want to thank our witnesses for sharing their thoughts with us today and I am confident that these ideas can help generate a bipartisan effort to improve the solvency of the Medicare program in the coming Congress.

## OPENING STATEMENT OF HON. FRANK PALLONE, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW JERSEY

Mr. PALLONE. Thank you, Mr. Chairman.

And good morning to everyone. It is good to be back after the election and seeing that our subcommittee is having hearings and moving forward in the lame duck as well as for next year.

While the total cost of healthcare fraud is difficult to obtain, estimates range anywhere from $65 billion to $98 billion annually. For every dollar put into the pockets of criminals, a dollar is taken out of the system to provide much-needed care to millions of seniors.

Fraud schemes come in all shapes and sizes and affect all kinds of insurance, public and private alike. Whether it is a sham storefront posing as a legitimate provider or legitimate businesses billing for services that were never provided, it is all the same result: undermining the integrity of our public health system and driving up healthcare costs.

I think we can all agree that healthcare fraud is a serious long-standing problem that will take aggressive long-term solutions to reverse. And we made a strong commitment to combat these issues within the Affordable Care Act. The law contains over 30 antifraud provisions to assist CMS, the OIG, and the Justice Department in identifying abusive suppliers and fraudulent billing practices. These include enhanced background checks, new disclosure requirements, onsite visits to verify provider information, and a requirement that healthcare providers create their own internal compliance programs.

The most important provisions in the Affordable Care Act change the way we fight fraud by heading up the bad actors before they strike and thwarting their enrollment into these Federal programs in the first place. And this way, we aren't just left chasing a payment once the money is already out the door.

And I am encouraged by the work that has been done of late. Over the past 3 years, the government has recovered a record-breaking $10.7 billion of healthcare fraud. So I am confident that we will begin to see even more savings as the implementation of these programs continues.

But our efforts must not stop there. Fraud is ever-changing; criminals will always find loopholes. And it is our job to keep one step ahead of them. Today we are going to hear from an array of witnesses about the state of antifraud measures currently being used, as well as discussing new approaches.

One example of a new approach is the secure ID program, which would create identification cards with encrypted chips. Each Medicare provider and beneficiary would be required to swipe these cards at the point of service.

And while there may be some benefits to this technology, such as preventing identity theft, I do have questions about how this would affect the overall system. Most important to me is how such a program would affect patients' access to care. For example, what happens if a senior simply forgets his ID card? Will he be sent away? I am also interested in how this technology can prevent the sheer criminals colluding with beneficiaries and handing out kickbacks.

And as we discuss any potential pilot programs, we must ensure that we can evaluate different technologies that allow us to determine what provides the best value for our tax dollars.

So, Mr. Chairman, as Congress discusses the expiring tax policies and impending sequestration during the lame duck, I do not believe we need to decrease benefits to seniors or raise the eligibility age to further fortify the program. Instead, we should focus on building upon the reforms of the ACA and creating better efficiencies within the system, including innovative ways to combat fraud and waste.

Standing up to protect Medicare includes supporting the constant work that must be done to cut waste, fraud, and abuse. And I am committed to working with my colleagues now and in the future to help address this ongoing threat. So I do appreciate your having this committee hearing today because I think it addresses a very important issue, both now and in the future, in the next Congress as well.

I did want, Mr. Chairman, if I could, to ask unanimous consent to insert two pieces of testimony in the record. The first is from the American Medical Association, which I believe raises some very important questions about smart cards. At a minimum, further discussion with a more robust representation of interested parties would seem to be warranted on that issue.

And the second is a statement from the National Health Law Program, which discusses smart cards in the Medicaid context and raises concerns about whether these cards could serve as a barrier to timely patient care.

So I would ask unanimous consent. I think you have both of them.

Mr. PITTS. Yes. Without objection, so ordered.

[The information follows:]

**STATEMENT**

**of the**

**American Medical Association**

**to the**

**Subcommittee on Health**
**Committee on Energy & Commerce**
**United States House of Representatives**

**Re: Examining Options to Combat Health Care Waste, Fraud and Abuse**

**November 28, 2012**

The American Medical Association (AMA) is pleased to provide the Committee on Energy & Commerce, Subcommittee on Health with our perspective on health care fraud and abuse.

*Recommendations to Combat Fraud & Abuse*

Physicians are firmly committed to eradicating fraud and abuse from the federal health care programs. Monies that inappropriately flow from federal health care programs divert vital resources that should be devoted to patient care. The AMA has long believed that the most efficient way to combat fraud is to employ targeted, streamlined methods of fraud identification and enforcement, rather than overly burdensome requirements for all physicians, the majority of whom strive to comply with the rules and regulations governing participation in the Medicare program.

The AMA recently published a white paper entitled *Medicare and Medicaid Program Integrity: Recommendations for Greater Value and Efficiency*. (Attached) As we explain in more detail therein, we recommend the following multi-pronged approach to combat fraud and abuse in health care in an efficient and cost-effective way:

- Move beyond the historic "pay and chase model" to a methodology that utilizes responsibly developed data analytics to enable targeted, clinically-informed fraud identification and prevention.

- Streamline and integrate federal and state program integrity initiatives and audits to produce impactful results.

- Increase oversight of federal and state government contractors to ensure that taxpayer funds are utilized in a cost-efficient manner.

- Avoid improper payments before they occur by placing a greater emphasis on physician education and outreach.

- Develop and test innovative solutions to decrease overall costs to the health care system by minimizing administrative burden and targeting law enforcement resources.

*Smart Cards*

We understand that the adoption of Medicare smart cards has been suggested as a means to combat fraud and abuse, and that the Committee is considering this avenue. Before moving forward with Medicare smart cards, we urge Congress to work with stakeholders, including practicing physicians, to carefully examine whether Medicare smart card proposals are appropriate and workable. While the AMA believes that technology that provides physicians with accurate and real time verification of patient eligibility, co-payment and remaining deductible information, and claims processing could prove to simplify the administrative process and reduce costs, we are concerned that proposals to adopt Medicare smart card technology in the near term could be counterproductive and place undue burdens on patients and physicians.

Adoption of Medicare smart card technology would have significant implications for administrative and claims workflow, and would require robust, burdensome operational and infrastructure changes for physician practices. Congress should therefore consider any proposal to proceed with Medicare smart card technology in light of the myriad regulatory requirements already facing physician practices. We are particularly concerned with proposals that would grant the Secretary of the Department of Health & Human Services broad discretion to implement Medicare smart cards by mid-2014. This is the same period of time in which physicians will be required to adopt ICD-10, and to meet other regulatory requirements, including those for the meaningful use electronic health record program, the Physician Quality Reporting System (PQRS), and the value-based payment modifier—programs that include financial penalties. The confluence of these requirements could be crippling for physician practices who are already struggling to meet numerous regulatory deadlines that require financial investment in their practices, have a significant impact on their office workflow, and put them at risk for multiple penalties.

**Before Congress acts further on Medicare smart card legislation, we strongly recommend that Congress convene a forum for stakeholder feedback, including the AMA, beneficiary groups, private payers, the Centers for Medicare & Medicaid Services (CMS), and standards organizations to delve into the multitude of administrative and technical ramifications that smart cards or other identity verification technologies would have for Medicare patients, physicians, and other providers.**

*Conclusion*

Thank you for the opportunity to provide our statement for today's hearing. We look forward to working with the Committee to identify efficient and cost-effective means to combat health care fraud and abuse. Should you have any questions concerning this statement, please contact Dana Lichtenberg, Assistant Director, Congressional Affairs, at dana.lichtenberg@ama-assn.org or (202) 789-7429.

# MEDICARE AND MEDICAID PROGRAM INTEGRITY RECOMMENDATIONS FOR GREATER VALUE AND EFFICIENCY

AMERICAN MEDICAL ASSOCIATION*

November 2012

## Executive Summary

The AMA and its physician members are firmly committed to eradicating fraud and abuse from health care. The following multi-pronged approach can reach this goal in an efficient and cost-effective way:

- Move beyond the historic "pay and chase model" to a methodology that utilizes responsibly developed data analytics to enable targeted, clinically-informed fraud identification and prevention.
- Streamline and integrate federal and state program integrity initiatives and audits to produce impactful results.
- Increase oversight of federal and state government contractors to ensure that taxpayer funds are utilized in a cost-efficient manner.
- Avoid improper payments before they occur by placing a greater emphasis on physician education and outreach.
- Develop and test innovative solutions to decrease overall costs to the health care system by minimizing administrative burdens and targeting law enforcement resources.

Many stakeholders, including physicians, patients, hospitals and other providers, law enforcement, legislators, and regulators share the goal of rooting out fraud and abuse from health care. While Congress, federal agencies, and the states have recently made unprecedented investments in improving health care program integrity, significant challenges remain. This white paper seeks to serve as a resource for all stakeholders as they consider how to more effectively combat fraud and abuse.

## Introduction

Financial losses due to health care fraud are estimated to range from $75 billion to $250 billion a year.[1] In the area of Medicare improper payments, the Centers for Medicare & Medicaid Services (CMS) estimate that $34.3 billion is misspent annually.[2] While there is an important distinction between fraud and *waste*, which often results from inadvertent coding or documentation errors, these numbers are far too high.[3]

Efforts to fight health care fraud, or to identify areas of waste, have a tangible impact on physician practices. To comply with anti-fraud rules and regulations, physicians proactively conduct internal audits and adopt compliance programs at their own cost.

When a federal or state audit is initiated, physicians often face significant costs to respond to medical documentation requests, consult with external accountants and attorneys, and navigate the appeals process. A recent survey estimated that the cost of appealing an audit was $110 *per claim*, with additional costs for complying with auditor requests for records and time spent.[4] Even in cases where auditors do not find fraud or improper billing, these costs are never recovered by physician practices.

Broad brush regulations that impose burdens on all providers, rather than focusing on those providers who have demonstrated a propensity to commit fraud or abuse, inequitably affect physicians and providers who are good actors, and result in unnecessary costs to the health care system.

**Data Analytics**

In the area of fraud identification, the utility of data analytics, or "predictive modeling," is increasingly coming to the fore.

The "pay and chase" model for fraud identification has been widely criticized as inefficient. Under "pay and chase," law enforcement and the federal health care programs spend resources pursuing claims that have already been paid. This approach puts fraud enforcers in the position of tracking down fraudsters and stolen funds *after the fact*, which is particularly challenging in cases where crime rings or international actors are involved.

The federal health care programs and law enforcement are now moving to a "fraud prevention" model that utilizes data analytics to identify aberrant claims in real time, and cross references such claims with other data sets to recognize fraudulent activity. This focused, streamlined approach, if clinically-informed and carefully developed, has the potential to prevent funds from being fraudulently misappropriated from the health care system.

Importantly, data analytic systems also have the potential to decrease the administrative burden that has traditionally accompanied the "pay and chase" model. The concept is that if fraud enforcers and those that oversee the federal health care programs can identify and prevent fraud on the front end, then post-payment activities, which have historically inequitably impacted many non-fraudulent physicians and other providers, may be minimized.

Implicit in the success of data analytics in fraud identification is the ongoing clinical input of physicians. Such expertise is required to enable data analytic systems to operate properly and reach a zero false positive rate. While federal program integrity regulators have described Medicare claims data analysis systems as "similar to technology used by credit card companies,"[5] the methodologies are dissimilar in that medical claims data analysis requires complex clinical knowledge. Just as appropriate claims coding and documentation implicate complicated clinical issues that require clinical acumen, review or analysis of such claims also necessitates the clinical lens of physician education and training.

Section 4241 of the Small Business Jobs Act of 2010[6] authorizes the Secretary of the Department of Health and Human Services (HHS) to use predictive modeling and other analytics technologies to identify improper claims for reimbursement and to prevent the payment of such claims under the Medicare fee-for-service program. In 2011, CMS implemented a data analytics system for fraud prevention, and is currently developing and refining the system's algorithms. Importantly, CMS has committed to working closely with clinical experts across the country and from every provider specialty to develop and refine algorithms that reflect the complexities of medical billing.

**To maximize the accuracy and effectiveness of CMS' data analytics system for fraud investigation, CMS should formalize a process for ongoing, independent clinical review of its data analytics system.**

**Audit Integration**

Physicians today face a voluminous number of federal and state auditors. Currently CMS contracts with Zone Program Integrity Contractors (ZPICs), Comprehensive Error Rate Testing (CERT) contractors, Medicare Recovery Auditors (Medicare RACs), Medicaid Recovery Audit Contractors (Medicaid RACs), Program Safeguard Contractors (PSCs), Payment Error Measurement Rate (PERM) Contractors, Medicaid Integrity Contractors (MICs), Medicare Administrative Contractors (MACs), and others.[7]

While some of these programs have unique functions, there is considerable overlap and duplication among them. The same claim may be subject to a Medicare RAC audit, a MAC audit, and a CERT audit, and there are few safeguards to ensure that the same claim—and the same physician—is not concurrently audited by multiple entities.

Physician confusion often accompanies an audit request because even though many of these contractors have the same goal—the identification of fraud or improper payments—audit contractors largely employ divergent operational guidelines and standards. The appeals processes, documentation limits, and look back periods vary among audit contractors.

For example, while the Medicare RACs may not request more than 10 medical records in a 45-day period for small physician practices, the MACs have discretion to require an unlimited number of medical records. And, while the Medicare RACs have similar appeals processes to the MACs, each Medicaid RAC has a different appeals process.

Consequently, physicians spend a great deal of time determining which contractor is auditing them, under what authority, and what the guidelines are for response. This confusion and misspent time unduly burdens physicians and contravenes the swift recoupment of improper payments to the federal government.

In direct response to a request by the AMA, and in response to this inefficiency, CMS has committed to undertake an "Audit of Audits" to review the myriad federal audit contractors and identify areas of duplication. This effort is strongly supported by the AMA.

**To alleviate physician confusion and best utilize federal funding, the result of CMS' "Audit of Audits" should be a reduction in duplicative program integrity audits for physicians and the adoption of streamlined audit policies and procedures.**

**Contractor Oversight**

In addition to an overall reduction in the number of federal program integrity audits, the contractors that conduct these audits should be subject to vigorous CMS oversight. While the AMA has worked productively with CMS program integrity audit staff, in general, it appears that many contractors proceed without sufficient CMS guidance or ongoing supervision.

For example, in June 2012, the Government Accountability Office (GAO) reported that over a five year period, the MIC contractors cost $102 million and returned less than $20 million, resulting in an overall loss to the federal government of $82 million.[8] Following this report, CMS committed to end the contracts of three of the five MIC contractors. While we welcome CMS' response, this report is very troubling and signifies that there is a lack of appropriate oversight by CMS of program integrity auditors.

*RACs*

In particular, physicians continue to have concerns about the Medicare and Medicaid RAC programs. The programs' contingency fee structure inappropriately incentivizes the RACs to conduct "fishing expeditions" that are exceedingly burdensome to physician practices. Physicians who seek to comply with RAC audits spend a significant amount of time and money to produce documents and appeal erroneous RAC determinations.

The RACs are also often inaccurate: CMS' FY2010 Recovery Auditor Report to Congress reported that 46 percent of the Medicare RAC determinations appealed were decided in the provider's favor.[9] This number is far too high. These errors result in needless expense for Medicare appeals tribunals and physicians. To promote efficiency and the best use of federal funds, greater oversight of RAC contractors and safeguards for physicians are needed.

The Medicaid RAC program also suffers from a lack of CMS supervision and transparency due to the complexity of running a program across all 50 states. While most states have finalized Medicaid RAC contracts, many states encountered operational, state-specific issues along the way that led to delays. Consequently, to date, there is no CMS resource where a physician can find information regarding what issues the Medicaid RAC in their state is permitted to audit.

These issues highlight the complexities associated with enacting national audit programs across all 50 states and should be understood by policy makers when utilizing federal auditors for Medicaid claims.

**To decrease inaccuracy, the RACs should be subject to a penalty for incorrect overpayment determinations. To reduce improper payments before they occur, the RACs should be incentivized to educate physicians regarding common payment errors.**

*Education*

An essential function of any program integrity auditor is physician education. Heretofore, CMS has largely employed listservs or transmittals to relay areas or issues prone to improper coding or documentation to physicians. To have greater impact, CMS should develop innovative, dynamic approaches to program integrity education, because such education can be a first line of defense against improper payments.

One such method of physician education is the employment of physician Contractor Medical Directors (CMDs). CMDs facilitate clinical-based discussions and serve as a bridge between physicians and federal programs on coverage and coding matters. Physician CMDs are a valuable resource for physicians to obtain education about Medicare's payment and coverage policies, and a venue for physician-to-physician discussion of Medicare policies that impact patient care.

However, the interaction between physicians and CMDs has been inhibited by the overall reduction of CMDs. Since the transition from carriers and fiscal intermediaries to the MACs, and the subsequent reduction of the number of MACs nationwide, the number of CMDs at the MAC-level has also decreased, leading to confusion in the medical community.

**CMS should develop innovative approaches to meaningful physician education. To further strengthen the role of the CMD as communicator, CMS should require a minimum of one physician CMD per state who is devoted to Medicare Part B issues for each program integrity audit program, unless a state medical society decides that a regional, multi-state CMD is appropriate.**

**Additional Solutions**

*Smart Cards:* Stakeholder feedback is imperative to understand the multitude of administrative and technical ramifications of smart cards or other identity verification technologies. While the AMA is poised to work with stakeholders to identify appropriate technologies for accurate verification of patient eligibility, adoption of smart card technology would have significant implications for administrative and claims workflow that must be carefully examined.

*Law Enforcement Access to Claims Data*: Currently, law enforcement agencies have access to Medicare claims data to investigate and prosecute fraud. Because these agencies have expertise in fraud investigation, their access to Medicare claims data is an appropriate and vital tool for fighting fraud. Some law enforcement agencies report that they have had difficulty in analyzing Medicare claims data because they receive the data too late to effectively investigate and pursue leads. To enable swift fraud investigation, law enforcement agencies should have access to Medicare claims data in real time.

*Increased Outreach from CERT Contractors:* In February 2011, the Office of Inspector General of the Department of Health and Human Services (HHS/OIG), published a report showing that, if the CERT contractor had increased outreach to physicians and other providers when conducting CERT audits, the HHS improper payment rate would have been decreased by 34 percent.[10] CMS should heed this report and ensure that its CERT contractors are conducting appropriate outreach and not unwittingly inflating the improper payment rate.

*Consistency among Prepayment Requirements*: Prepayment and prior authorization requirements can be burdensome for physicians because payers require varied and disparate administrative documentation and addenda. Any proposals to employ prepayment or prior authorization must examine the administrative burdens and impact on patient care of such programs prior to adoption. For example, a recent AMA survey showed that nearly two-thirds (63%) of physicians typically wait several days to receive preauthorization from an insurer for tests and procedures, while one in eight (13%) wait more than a week.[11] Proposals that address prepayment review or prior authorization should be focused on extreme statistical outliers and should be informed by the clinical knowledge and ongoing input of physicians with expertise in the procedure or service in question prior to development and throughout implementation.

*Wheelchair Advertisements:* Deceptive advertisements that promise "free" wheelchairs "paid for by Medicare," and assure seniors that they will be covered for such supplies, do not promote program integrity. Physicians have reported patient inquiries regarding such advertisements, and some incidences of "physician shopping" by seniors—at the urging of wheelchair suppliers—to solicit a wheelchair order. Advertisements by wheelchair suppliers should be subject to greater oversight.

*HEAT Teams:* Over the last few years, HHS, the Department of Justice (DOJ), and state law enforcement agencies have teamed up to work in a collaborative manner on fraud investigations via Health Care Fraud Prevention and Enforcement Action Teams (HEAT). The result has been an increase in fraud prosecutions and a greater recoupment of funds to the federal government. This targeted, focused method of investigation should continue to be supported by stakeholders.

*Home Health Company Bundles:* Home health companies are increasingly utilizing "bundled" service orders wherein a physician cannot elect to order individual services for a beneficiary, but instead, may only order a bundle of several services. This practice puts physicians in the untenable position of either not ordering individual services because they are bundled with non-necessary services, or trying to make clear to the home health company that the order only applies to some of the services in the bundle. Home health companies should accord physicians the discretion to order the individual, specific services that are medically necessary for the beneficiary.

*Program Integrity Law Waivers:* The "program integrity laws" (e.g., the Ethics in Patient Referrals Act, the federal anti-kickback statute) may be inappropriately triggered by new efforts to improve quality and lower costs . For example, a physician who shares savings with a team of other providers may violate the federal anti-kickback law. Or, a physician who provides services like care management or telephone consultations may implicate the civil monetary penalty prohibiting beneficiary inducements. These laws must be addressed for innovative payment and delivery reforms to succeed.

**Conclusion**

The AMA is committed to engaging with other stakeholders going forward to identify and inform focused and efficient program integrity measures. Clinically-developed data analytics systems, streamlined and integrated audits, increased contractor oversight, a greater emphasis on physician education, and the additional solutions discussed in this white paper can produce cost-efficient results that decrease physician burden and increase savings.

* The American Medical Association is a national physician and medical student member organization whose mission is to promote the art and science of medicine and the betterment of public health.

[1] National Health Care Anti-Fraud Association. Statement of Louis Saccoccio, Executive Director, on "Improving Efforts to Combat Health Care Fraud," before the U.S. House Committee on Ways and Means, Subcommittee on Oversight. March 2, 2011. Available at http://waysandmeans.house.gov/UploadedFiles/Socc.pdf.

[2] The most recent Medicare Fee-for-Service Improper Payment Report was released in 2011, and reported on improper payments in 2010. See Centers for Medicare & Medicaid Services. *Medicare FFS 2010 Improper Payment Report.* Available at http://www.cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/CERT/Downloads/Medicare_FFS_2010_CERT_Report.pdf.

[3] The term "waste" refers to improper payments unrelated to fraud. According to the Government Accountability Office, an improper payment is any payment that should not have been made or that was made in an incorrect amount (including overpayments and underpayments) under statutory, contractual, administrative, or other legally applicable requirements. This definition includes any payment to an ineligible recipient, any payment for an ineligible good or service, any duplicate payment, any payment for a good or service not received (except where authorized by law), and any payment that does not account for credit for applicable discounts. See *Improper Payments Elimination and Recovery Act of 2010*, Pub. L. No. 111-204, § 2(e), 124 Stat. 2224, 2227 (codified at 31 U.S.C. § 3321 note). GAO cite available at http://www.gao.gov/assets/600/591601.pdf. Page 1.

[4] Frank Cohen, MPA, MBD. *Survey on Recoupment: March 10 through March 25, 2012.* (April 11, 2012). Available at http://www.frankcohengroup.com/Surveys.aspx.

[5] Centers for Medicare & Medicaid Services. *Predictive Modeling Analysis of Medicare Claims.* Available at http://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNMattersArticles/downloads/SE1133.pdf.

[6] 42 U.S.C. 1320a-7m.

[7] Centers for Medicare & Medicaid Services. *Contractor Entities At A Glance: Who May Contact You About Specific Centers for Medicare & Medicaid Services (CMS) Activities.* Available at http://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/downloads/ContractorEntityGuide_ICN906983.pdf.

[8] Government Accountability Office. *National Medicaid Audit Program: CMS Should Improve Reporting and Focus on Audit Collaboration with States.* (GAO-12-627). July 2012. Available at http://www.gao.gov/assets/600/591601.pdf.

[9] Centers for Medicare & Medicaid Services. *Implementation of Recovery Auditing at the Centers for Medicare & Medicaid Services. FY 2010 Report to Congress as required by Section 6411 of the Affordable Care Act.* Available at https://www.cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/recovery-audit-program/downloads/FY2010ReportCongress.pdf.

[10] Centers for Medicare & Medicaid Services. *Pilot Project to Obtain Missing Documentation Identified in the Fiscal Year 2010 CERT Program* (A-01-11-00502).

[11] American Medical Association Survey of Physicians on Preauthorization Requirements. May 2010. Available at http://www.ama-assn.org/ama1/pub/upload/mm/399/preauthorization-survey-highlights.pdf.

## *TESTIMONY BEFORE THE COMMITTEE ON ENERGY AND COMMERCE*

## SUBCOMMITTEE ON HEALTH

### FOR THE HEARING ENTITLED "EXAMINING OPTIONS TO COMBAT HEALTH CARE WASTE, FRAUD, AND ABUSE"

### NOVEMBER 28, 2012

### BY THE

## NATIONAL HEALTH LAW PROGRAM

The National Health Law Program ("NHeLP") submits this testimony to the Energy and Commerce Committee's Subcommittee on Health. NHeLP protects and advances the health rights of low-income and underserved individuals. The oldest non-profit of its kind, NHeLP advocates, educates and litigates at the federal and state levels. NHeLP's testimony addresses the use of "biometrics" for identity verification purposes in Medicaid.

Biometric technology compares an individual's physical features (e.g., fingerprint, palm, iris) to information saved in a central database to verify that individual's identity. In 2011, several state legislative proposals involved the implementation of biometric smart cards to verify the identity of Medicaid beneficiaries. Proponents for the use of biometrics in Medicaid believe this technology addresses both beneficiary fraud (by preventing card-sharing with non-enrollees), and provider fraud (by reducing phantom-billing and other forms of fraud). Yet, past experience has shown that verification programs for government benefits do not effectively reduce fraud or save money, but rather serve as a barrier to enrollment. NHeLP's testimony will:

1) demonstrate how biometric proposals create barriers to enrollment and care,
2) highlight how these proposals are a costly and misguided effort to address fraud,
3) explain the Centers for Medicare & Medicaid Services' (CMS)' position on finger-imaging and other similar procedures, and
4) analyze the legality of biometric smart card proposals.

**Barriers to Enrollment and Care**

The stated aim of biometric programs is to reduce costs by reducing fraud. However, the evidence to date shows that identity verification programs reduce costs by discouraging eligible beneficiaries from obtaining benefits rather than by preventing fraud.

State legislative proposals in 2011 to replace existing Medicaid cards with biometric smart cards required the collection of biometric data (fingerprint, palm scan, etc.) to be stored in a central database. The proposals also required the installment of biometric fingerprint or palm scanners, as well as card readers in provider's offices, hospitals, and pharmacies, with the intent that Medicaid beneficiaries provide biometric proof of identity before receiving services and again at the completion of care or services.

If a state makes the collection of biometric data part of the Medicaid application process, this means that in addition to submitting an application, Medicaid applicants will have to go into a county social service office or other location to have this data collected. If the requirement applies to current beneficiaries as well, they would have to do the same. For some people, this additional hurdle will make it difficult to apply for Medicaid and keep those benefits. This will particularly be true for seniors and people with disabilities.

Moreover, past experience has shown that identity verification programs save money by keeping eligible beneficiaries away. In 1995, New York began requiring all public assistance beneficiaries to have their fingerprints, signature, and photograph taken at a local social service facility before the state would issue any benefits. In the first two years of the program, more than 38,000 beneficiaries lost public assistance benefits for not submitting biometric samples, saving the state $297 million.[1] Yet most of the individuals did not submit samples because they were either "unaware of the requirement, did not understand it, or were unable to meet the compliance deadline."[2] The state later reinstated benefits for most of these beneficiaries.[3]

Five years later (in 2000), New York required adults qualifying for Medicaid to enroll in its public assistance biometric system due to concerns of identity fraud.[4] However, the state terminated this requirement in 2008 because it was becoming increasingly difficult to obtain biometric data from Medicaid beneficiaries (since in-person applications were no longer required), and there was lack of evidence that the program reduced Medicaid fraud.[5] At a time when online applications are more prevalent, and the Affordable Care Act (ACA) specifically encourages states to streamline their application processes and simplify eligibility requirements to make it easier for people to get benefits, biometric smart card proposals are counter-productive and create barriers to enrollment and care.[6]

**Costly and Misguided Effort to Address Fraud**

[1] DEP'T OF MEDICAL ASSISTANCE SERV., VIRGINIA MEDICAID BIOMETRIC PILOT IMPLEMENTATION REPORT, H. Doc. 2010-10, Reg. Sess., at A-4 (2010), *available at* http://leg2.state.va.us/dls/h&sdocs.nsf/By+Year/HD102010/$file/HD10.pdf.

[2] *Id.* at A-5.

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] ACA § 1413, 42 U.S.C. 18083.

Biometric smart card proposals also are expensive to implement. In Georgia, a proposal for a statewide rollout to replace existing Medicaid cards with biometric smart cards was estimated to cost approximately $23 million for the first year.[7] Similarly, in New York a proposal to establish a "Medicaid identification and anti-fraud biometric technology program" was estimated to cost $20 million.[8] Yet, the savings under these programs are unclear, and their effectiveness questionable. Texas was one of the first states to use biometric finger-imaging in Medicaid.[9] In 2004, the state implemented the Medicaid Integrity Pilot (MIP).[10] At the conclusion of the pilot, Texas was unable to determine the extent to which the MIP reduced beneficiary fraud, in part, because it had not determined the extent to which this type of fraud occurred prior to the pilot.[11] Nevertheless, in 2006, Texas implemented the Medicaid Access Card (MAC) program, which was a mandatory smart card/biometric identification program for Medicaid beneficiaries and providers in three counties.[12] While the program was scheduled for statewide implementation in 2008, Texas dropped the fingerprint component after federal officials questioned its cost-effectiveness.[13]

Moreover, it is estimated that only ten percent of health care fraud is attributable to consumers, while eighty percent is committed by medical providers and ten percent by others, such as insurers and their employees.[14] In addition, "card-sharing" has never been proven to be a widespread problem in the Medicaid program. For example, in March 2011, during legislative hearings, the Inspector General for Georgia's Department of Community Health indicated that in the past two and a half years, there were only five reports of someone trying to use another person's Medicaid card and only three of those reports were substantiated.[15]

Those in favor of biometric technology claim it can also help stop provider fraud by reducing phantom-billing and other forms of fraud. Yet, these biometric programs place the burden on Medicaid beneficiaries to catch dishonest providers. Less costly and more effective methods of uncovering provider fraud exist. For example, by investing more money in Medicaid Fraud Control Units (MFCUs) rather than in biometric technology, states can obtain greater financial

[7] Letter from Russell W. Hinton, Georgia State Auditor, Dep't of Audits and Accounts, to Honorable John Albers, Georgia State Senator (Feb. 25, 2010) (on file with author).

[8] S. 4384, 199th Reg. Sess. (N.Y. 2011) (as introduced Apr. 4, 2011), *available at* http://open.nysenate.gov/legislation/bill/S4384-2011.

[9] Carrie Teegardin & Christopher Quinn, *Medicaid smart card idea raises questions*, ATLANTA JOURNAL-CONSTITUTION, Mar. 25, 2011, *available at* http://www.ajc.com/news/georgia-politics-elections/medicaid-smart-card-idea-885664.html.

[10] DEP'T OF MEDICAL ASSISTANCE SERV., *supra* note 1, at A-5.

[11] *Id.* at A-6.

[12] *Id.*

[13] Teegardin & Quinn, *supra* note 9.

[14] Sara Rosenbaum et al., George Washington University Department of Health Policy, Health Care Fraud 14 (2009), *available at* http://www.rwjf.org/files/research/50654.pdf.

[15] Teegardin & Quinn, *supra* note 9; *see also* GEORGIA COUNTY WELFARE ASSOC., REPORT ON THE 2012 SESSION OF THE GEORGIA GENERAL ASSEMB., 10 (2011) *available at* http://www.gcwa.us/documents/Reporton2011Legislation.pdf.

resources to combat fraud and can achieve greater cost savings by addressing provider fraud (the most prevalent type of fraud) .[16] The MFCU budget for an individual state is generally funded with federal grants on a 75 percent matching basis.[17] MFCUs conduct a statewide program for the investigation and prosecution of health care providers that defraud Medicaid, yet states only spend a small percentage of their Medicaid budget on their MFCUs, even though recovery amounts can be significant.[18]

**CMS' position on finger-imaging and other similar procedures**

In 2001, CMS (then called the Health Care Financing Administration or HCFA) clarified federal policy on the use of finger-imaging or similar procedures as part of states' Medicaid programs.[19] According to CMS, for a state to use finger-imaging procedures, it must demonstrate that these procedures will be:

- cost effective and efficient in addressing a particular identified problem,
- administered in a way that will minimize deterrents to enrollment and ongoing access to benefits for eligible individuals, and
- more effective than other procedures.[20]

CMS also requires that a state show it has explored alternatives to address the identified problem that might have less of a deterrent effect and has determined that imaging procedures are superior to those other procedures.[21]

Also, in any demonstration of cost-effectiveness and efficiency, the state must base anticipated savings on reasonable projections of savings to be achieved due to fraud detection and "not savings likely to be achieved because eligible families and individuals are deterred from applying for or retaining Medicaid coverage as a result of the procedures."[22] Finally, CMS says that states will have to demonstrate that other, less intrusive, procedures would not adequately

[16] While increasing MFCU resources and workforce may produce substantial cost-savings, it is important to make sure MFCUs are not denying or aggressively contesting Medicaid reimbursements for providers who perform legitimately rendered services.

[17] NATIONAL ASSOCIATION OF MEDICAID FRAUD CONTROL UNITS, MEDICAID FRAUD CONTROL UNITS, http://www.namfcu.net/about-us/about-mfcu (last visited Nov. 25, 2012).

[18] OFFICE OF INSPECTOR GENERAL, U.S. DEP'T OF HEALTH & HUMAN SERVICES, MFCU STATISTICAL DATA FOR FISCAL YEAR 2011, (2011), http://oig.hhs.gov/fraud/medicaid-fraud-control-units-mfcu/expenditures_statistics/fy2011-statistical-chart.xlsx (last visited Nov. 25, 2012).

[19] Memorandum from Cindy Mann, Director, Family and Children's Health Program to Health Care Financing Administration Associate Regional Administrators (April 4, 2001) (on file with author).

[20] *Id.*; *see also* GERALD FRALICK, NORTH CAROLINA CHIEF INFO. OFFICER, SMART CARD INITIATIVE: QUARTERLY REPORT TO THE JOINT LEGISLATIVE OVERSIGHT COMMISSION ON INFORMATION TECHNOLOGY, at 5 (Jan. 2011), *available at* https://www.scio.nc.gov/library/pdf/Smart_Cards_report_%28January_2011%29_FINAL.pdf.

[21] Mann, *supra* note 19.

[22] *Id.*

address the problem and that the state will implement the technology in a manner that is not likely to deter eligible individuals from applying for or continuing to receive benefits.[23]

Biometric proposals are likely to deter eligible individuals from applying for or continuing to receive benefits by stigmatizing Medicaid beneficiaries. Having Medicaid beneficiaries scan their fingerprint or palm every time they go in and out of a provider's office, hospital or pharmacy targets Medicaid beneficiaries by making them stand out in public settings. Only Medicaid beneficiaries will be required to do this, adding to any stigma that may already exist about receiving government benefits. As indicated in a report by Virginia's Department of Medical Assistance Services, a negative public perception exists around fingerprints because they are used by law enforcement agencies, and using fingerprints to verify the identity of Medicaid beneficiaries will intimidate people and keep them away from the Medicaid program and the health care services they need.[24]

**Legality of Biometric Smart Card Proposals**

To date, there appear to be no published cases where a court has ruled directly on the legality of biometric smart cards in Medicaid. However, courts have assessed state laws that impose substance abuse testing requirements for public assistance applicants and recipients. These cases provide helpful analogies to assess the validity of biometric proposals.

In *Marchwinski v. Howard*, the Sixth Circuit Court of Appeals affirmed a District Court decision holding that the suspicionless testing for substance abuse of public assistance applicants/recipients is an unconstitutional search and seizure under the Fourth Amendment of the U.S. Constitution.[25] The district court stated that "some quantum of individualized suspicion" is generally required for a search or seizure to be constitutional except in "certain limited circumstances" when "special needs" are shown.[26] The court further noted that the state had not demonstrated a special need that justified a departure from the requirement of "individualized suspicion" and failed to show that public safety was genuinely placed in jeopardy in the absence of substance abuse testing of all public assistance applicants and of random testing of public assistance recipients.[27]

Similarly, biometric data collection and verification based on a *belief* that applicants/recipients of the Medicaid program are committing fraud may also be considered an unconstitutional search and seizure. The collection of an individual's physical features (e.g., fingerprint, palm, iris)

[23] *Id.*
[24] DEP'T OF MEDICAL ASSISTANCE SERV., *supra* note 1, at 2-3. Other biometric options have other types of disadvantages, for example, iris imaging requires lengthy staff training, hand geometry requires a large amount of storage space to maintain data electronically, and palm vein imagining requires a certain amount of physical contact with biometric sensors, which may spread disease. *Id.*
[25] 60 Fed. App'x. 601, (6th Cir. 2003), *aff'ing* 113 F. Supp. 2d 1134 (E.D. Mich. 2000).
[26] *Id.* at 1138.
[27] *Id.* at 1139-1140.

compared to a central database each time the Medicaid beneficiary receives services is not much different from the collection and testing of a urine sample, which is considered a "search" within the meaning of the Fourth Amendment.[28] States have proposed to collect biometric data without an individualized suspicion of fraud, and simply believe "some" people in the Medicaid program are committing fraud. As in *Marchwinski*, there are no special needs showing a public safety concern that would justify a suspicionless search. Standards and methods for determining Medicaid eligibility must be consistent with rights of individuals under the U.S. Constitution and civil rights laws.[29] Therefore, if biometric data collection is a violation of the Fourth Amendment, it would be unconstitutional and could not be used as a standard for determining Medicaid eligibility.

In *Lebron v. Wilkins*, a district court granted a preliminary injunction finding that a Florida law requiring all Temporary Assistance for Needy Families (TANF) applicants to submit to suspicionless drug testing is highly likely to violate the Fourth and Fourteenth Amendments.[30] The plaintiff contended that the state's drug testing program violated his right to be free from unreasonable searches.[31]

As background to the case, in 1998, the Florida legislature enacted legislation that required the Florida Department of Children and Families to develop and implement a "Demonstration Project" to study and evaluate the impact of drug-screening and testing on TANF applicants' employability, job placement, job retention and salary levels, and make recommendations based, in part, on a cost-benefit analysis.[32] The recommendation at the end of the project was not to expand it because of the high costs of drug testing compared with the benefits derived, and the "minimal differences in employment and earnings between those who showed evidence of current substance abuse and those who did not."[33]

Yet in 2011 the Florida legislature "resurrected" the concept of drug testing TANF applicants.[34] No new studies were conducted, and no new data was offered. Nevertheless, on July 1, 2011, Florida began drug testing TANF applicants.[35] In the program's first month, preliminary results from drug testing showed that only 2% of applicants tested positive.[36] Applicants who did not take the drug test were denied benefits.[37] The district court mentions that some of these denials may be due to the statute's deterrent effects, for example: inability to pay for the drug test, lack of "approved" laboratories near the applicant's residence, inability to secure transportation to a

[28] *Marchwinski, supra* note 25.
[29] 42 C.F.R. § 435.901.
[30] 820 F. Supp. 2d 1273 (M.D. Fla. 2011).
[31] *Id.* at 1276.
[32] *Id.*
[33] *Id.* at 1278.
[34] *Id.*
[35] *Id.* at 1278,1280.
[36] *Id.* at 1280.
[37] *Id.* at 1281.

laboratory, or refusal to accede to what an applicant considers an unreasonable condition to receive benefits.[38] Ultimately, the court held the state had not shown evidence that any TANF funds would be saved by instituting the program, or that there would be any financial benefit or net savings due to the passage of the statute.[39]

In a very similar way, biometric smart card policies produce questionable cost-savings and cause the same deterrent effects. As explained more fully in the sections above, the evidence to date shows that identity verification programs reduce costs by discouraging eligible beneficiaries from obtaining benefits rather than by preventing fraud. This was the case in New York where tens of thousands of beneficiaries were removed from public assistance for not submitting biometric samples, and eventually this requirement was removed, in part, because of lack of evidence that the program reduced Medicaid fraud.[40]

**Conclusion**

Biometric smart card programs claim to reduce fraud and save state resources, yet they place an undue burden and stigma on Medicaid applicants and beneficiaries. Past biometric technology programs have not proven to be cost-effective and have deterred eligible beneficiaries from enrolling in the program and receiving services. The vast majority of Medicaid fraud is committed by providers, not beneficiaries, and there are other less costly ways to address provider fraud. Finally, the legality of biometric smart card proposals is questionable, and it appears the collection of biometric data in Medicaid would be considered unconstitutional.

For further information or questions about this testimony, please contact Michelle Lilienfeld at the National Health Law Program, (310) 204-6010 or lilienfeld@healthlaw.org.

[38] *Id.*
[39] *Id.* at 1290-1291.
[40] DEP'T OF MEDICAL ASSISTANCE SERV., *supra* note 1, at A-4, 5.

Mr. PALLONE. Thank you. And I yield back.

Mr. PITTS. The Chair thanks the gentleman and now recognizes the vice chairman of the subcommittee, Dr. Burgess, for 5 minutes.

## OPENING STATEMENT OF HON. MICHAEL C. BURGESS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. BURGESS. And I thank the chairman for the recognition and the time.

We all know that the Centers for Medicare and Medicaid Services has not done enough to address the issue of inappropriate payments even though our government-administered health system does appear to waste billions of dollars every year. Eliminating inappropriate payments, payments that, in fact, embarrassingly hemorrhage from the programs, is, as Mr. Pallone pointed out, a bipartisan issue.

Unfortunately, there is no simple answer. Fraud analysts are estimating up to 10 cents out of every dollar that is spent in health care is lost yearly to fraud. That is 10 cents out of every dollar we are spending. One-fifth of all healthcare expenditures in this country are spent on the Medicare system. So that is a big figure, a big dollar figure, that demands our attention. We could pay for everything we need to pay for, the doc fix, in this decade and the next decade if we simply fixed that problem.

We do pay providers in practically an automatic fashion. This May I asked for and received a briefing from one of the deputy administrators at CMS, who is the Director for Center Program Integrity, and talked about their efforts to move from a pay-and-chase mindset into one that builds on a system of predictive modeling.

Now, the good news is that things do seem to be moving forward in that arena. They started with 9 algorithms and quickly grew to over 30. And that was last May, so I don't know what that figure stands at today. But it is clearly an area that is crying to be taken care of.

They are some first steps, but they are not going nearly far enough. Had we addressed these technologies years ago, just think about the amount of money that could have been saved and how many generations of algorithms and new generations of algorithms that could now be in place.

As a physician, I support prompt pay, and I realize the size, scope, and complexity of the Medicare program makes it highly susceptible to inappropriate payments. We have to accelerate the use of these analytics to aid in our detection efforts. But, you know, it is not new concepts. The Visa folks do this every hour of every day of every week and will call you when there is untoward activity occurring on your credit or debit card and are pretty quick to do so. Unfortunately, in our Federal agencies, anything we do cannot be defined as "quick."

We have learned from watching some of the predictive modeling activities in the crop insurance program that, simply recognizing that there is a cop on the beat, people are less likely to misbehave. Right now we have whole industries—illicit industries, crooked industries—that are being built around the fact that we just simply make so much money available to them, they can hardly resist the temptation to cheat.

Back-end investigations will remain a part of what CMS is required to do. We need to be sure that we have the prosecutorial force to be able to go—when these individuals are uncovered, to make certain that we can go after them with the full force of the law.

The Government Accountability Office has made recommendations, some of which date back to a decade when I first started in Congress, and many of those have yet to be implemented. And we need to pay attention to what they tell us this morning.

Developing new and innovative approaches to fight fraud has become increasingly important. I certainly look forward—we have a very—a panel in front of us today that has vast experience, and I expect that they can give us a great deal of enlightenment.

And with that, I do want to yield to my colleague from Georgia, Dr. Gingrey.

[The prepared statement of Mr. Burgess follows:]

**Opening Statement**
**Hearing on "Examining Issues to Combat Health Care Waste Fraud and Abuse"**
**Subcommittee on Health**
**Congressman Michael C. Burgess**

Thank you Mr. Chairman,

CMS has not done enough to address fraud, even though our government-administered health systems needlessly waste billions each year.

Eliminating waste, fraud and abuse that embarrassingly hemorrhages from these programs is a bipartisan issue.

There isn't a silver bullet – but with fraud analysts estimating up to 10% of total health care expenditures are lost to fraud yearly – there is obviously more we can do.

Medicare spending currently represents about 21 percent of national health care spending.

Yet, we have traditionally paid providers in practically automatic fashion.

I have been briefed on CMS's efforts to move away from a pay and chase mindset into one that builds on predictive modeling.

As I long expected these programs are already proving to be innovative -- 9 original algorithms in just a few months have already grown to over 30.

While CMS has taken some first steps, they are not perfect.

Had we addressed these technologies years ago think how much money could have potentially been saved and how many generations of algorithms we could have learned from.

While I support prompt pay I realize the size, scope, and complexity of Medicare program makes it highly susceptible to waste, fraud, mismanagement, abuse, and improper payments and we need to accelerate the use of analytics to aid in our detection efforts.

The GAO and others have said these characteristics are "unsustainable" and GAO has placed Medicare on its "high risk" list since 1990.

However, back-end investigations will remain a part of what CMS does.

The GAO has made recommendations- some dating back as far as 2003 – which have failed to fully be implemented.

Developing new and innovative approaches to fight fraud has become increasingly important and I look forward to the testimony to determine how we can achieve this goal.

Thank you.

## OPENING STATEMENT OF HON. PHIL GINGREY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF GEORGIA

Mr. GINGREY. I thank Dr. Burgess for yielding to me.

Mr. Chairman, it is appropriate that we as a committee look at the various tools for fixing the Medicare program. Strategically, identifying fraud, waste, and abuse is essential to trying to solve and to save this program that so heavily benefits our seniors.

Let's face it, Medicare will go bankrupt, depending on who you talk to, between 2017 and 2024. At this point, we must seek to identify waste and eliminate it—an estimated, what is it, anywhere from $60 billion to $90 billion a year. And this money should be used to preserve Medicare and not pad the wallets of criminals.

We need to ensure that the agencies are all using all of the powers they already have at their disposal to save wasted money. I would hope that we can eventually take a proactive approach in identifying criminals, one where we eliminate the payment before it is made rather than chase them afterwards. This is a huge problem. And I think that every one of us are appalled, especially those of us who are healthcare providers, who have worked in that field, as Dr. Burgess and myself, for years, trying to do the right thing, and knowing that people are stealing money from those who really, really need it.

So I am glad, Mr. Chairman—thank you for having the hearing. And I look forward to hearing from the witnesses.

And I yield back. Thank you, Dr. Burgess.

Mr. PITTS. The Chair thanks the gentleman and now recognizes the ranking member of the full committee, Mr. Waxman, for 5 minutes for an opening statement.

## OPENING STATEMENT OF HON. HENRY A. WAXMAN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. WAXMAN. Thank you, Mr. Chairman, for recognizing me and for holding this hearing today and focusing on the important topic of Medicare and Medicaid fraud.

Healthcare fraud robs taxpayers of funds, affects the quality of care provided to program enrollees, and saps the public confidence in the program. And that is why I see fighting fraud as a critical need and an issue where we should be able to achieve bipartisan consensus.

The vast majority of Medicare and Medicaid providers are compassionate and honest. The vast majority of beneficiaries of these programs desperately need the care they provide. So we need to be tough on fraud and tough on criminals who take advantage of these programs and their beneficiaries, but we can and should not blame the victim.

One of the reasons I am so proud of the Affordable Care Act is that it contains dozens of antifraud provisions. The legislation has the most important reforms to prevent Medicare and Medicaid fraud in a generation, and already they are yielding results.

As a result of the strengthened enrollment and re-enrollment process, CMS has deactivated 136,682 provider enrollments and revoked another 12,477. The new fraud prevention system of analytics has generated numerous new leads for new and existing investigations and providers and beneficiary interviews.

The healthcare reform law shifted the prevailing fraud-prevention philosophy from pay and chase, where law enforcement authorities only identify fraud after it happens, to inspect and prevent. But even so, the need for boots-on-the-ground investigation work will always remain.

I am proud of these efforts to reduce fraud. We are going to hear today from a number of witnesses describing additional steps and technologies CMS could take in terms of fighting fraud. I know some of today's witnesses support legislation to mandate CMS undertake a pilot project testing specific technology. If Congress is considering giving CMS additional funding to test new fraud-fighting activities, first we should give them the flexibility to test different interventions and compare the results, not mandate one very prescriptive activity.

Second, we must ensure that whatever CMS decides to test is evaluated carefully to determine which technologies provide the best value for our tax dollars. Smart cards may help address the problem of identity theft; however, reducing identity theft will not eliminate fraud, and smart cards may not be the only way to address issues of identity verification. In fact, both the American Medical Association, representing our Nation's physicians, and the National Health Law Program, representing low-income beneficiary advocates, raise some important issues for policymakers to consider with respect to these cards.

I am glad the committee is continuing the dialogue on reducing fraud in the Medicare program. If we truly care about protecting the taxpayer, we should build upon the administration's initiatives to reduce Medicare fraud. I hope that we can work across the aisle to do just that.

Thank you, Mr. Chairman. I yield back my time.

Mr. PITTS. The Chair thanks the gentleman.

That concludes our opening statements from Members.

Mr. BURGESS. Mr. Chairman?

Mr. PITTS. Yes?

Mr. BURGESS. If I could ask unanimous consent, I have a letter here from Mr. Roskam describing a bill that he and Mr. Carney have introduced on provider identity protection, and I would like to submit that for the record.

Mr. PITTS. Without objection, so ordered.

[The information follows:]

PETER J. ROSKAM
6TH DISTRICT, ILLINOIS

CHIEF DEPUTY WHIP

COMMITTEE ON WAYS AND MEANS

SUBCOMMITTEES:

SELECT REVENUE MEASURES

HEALTH

Congress of the United States
House of Representatives
Washington, DC 20515–1306

227 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-4561

150 S. BLOOMINGDALE ROAD
SUITE 200
BLOOMINGDALE, IL 60108
(630) 893-9670

roskam.house.gov
facebook.com/RepRoskam
twitter.com/PeterRoskam

I would like to thank Chairman Upton and Ranking Member Congressman Waxman for allowing me the opportunity to submit this statement for the record.

In the United States, over 100 million Americans rely on Medicare/and or Medicaid for their health care needs. And with 100,000 baby boomers added to the Medicare rolls each year, as well as an expansion of Medicaid under the president's health care law, these programs will only grow larger. While there has been heated debate over the future of Medicare in particular, and how to prevent its coming bankruptcy, we can all agree that the amount of Medicare and Medicaid dollars lost to waste, fraud and abuse also threatens the solvency of the program.

60 minutes, the Washington Post, and ABC News have all reported that Medicare loses roughly $60 billion each year due to fraud. The FBI has stated that the number may be closer to $250 billion and while these numbers are vastly different they all indicate that the system is broken.

For years the Centers for Medicare and Medicaid Services (CMS) have operated on a pay-and-chase model; meaning that they simply pay out for every claim that comes through their system. They are then left to later track down payments made in error and many times this money has already left the country.

To give an indication of the scale of payments, CMS currently processes nearly a billion claims a year and handles over 1.5 million providers. We routinely talk about how impressive it is that CMS has such a low overhead, considering the size and scope of their responsibilities. However, they have only recently really started to better monitor these claims and move away from pay-and-chase which we hope will better align their process with that of the private sector.

This is why I introduced bipartisan legislation in the House with my colleague from Delaware; Congressman John Carney aimed at cutting back on the fraud and abuse within Medicare and Medicaid. The FAST Act is sponsored in the Senate by Senators Tom Carper of Delaware and Tom Coburn of Oklahoma. Our legislation would help protect provider's identities so they are not incorrectly burdened with audits, require CMS to update their systems more frequently, and push CMS further along in their use of predictive modeling. Predictive modeling is used by credit card companies to determine if a purchase is fraudulent or questionable. The credit card industry processes $17 trillion in transactions a year and has only a .044% loss due to fraud and abuse. It is my hope that we can continue to work with the committee on moving this legislation forward.

CMS should be able to do the same with their payment system and question irregularities. The good news is CMS has instituted a predictive modeling system but with mixed reviews.

The Government Accountability Office (GAO) recently submitted a report to Congress commenting on CMS's implementation of their Fraud Prevention System (FPS). The GAO stated that the system is being used similarly to other state and private systems but the system needs better metrics to measure against.

CMS currently has no quantitative way to measure the system's effectiveness or outlined specific performance goals. The report also mentions that the system needs to be better integrated into other CMS systems in order to operate more efficiently. While it is good to know that CMS is moving ahead with the system it is disappointing to hear that it could be used more efficiently. It is my hope that they will take the suggestions of the GAO, of which they agreed on many of the recommendations, so that we can begin to stem the tide of losses at CMS.

While there may be issues that we here in Congress disagree on, I truly believe that we can work in a bipartisan matter to ensure that a program as crucial as Medicare is not eroded because of fraud that could easily be prevented. These are commonsense ideas that other sectors and private companies are employing that could be better used within CMS to stop the waste, fraud and abuse.

Mr. PITTS. Any other Members having opening statements, if you will provide them in writing, they will be made a part of record.

Today we have one panel with seven witnesses.

Our first witness is Ms. Kathleen King, director of the Health Care team at the U.S. Government Accountability Office. Our second witness is Mr. Dan Olson, director of fraud prevention at Health Information Designs. Third, Ms. Alanna Lavelle is the director of the East Region/Special Investigations Unit at WellPoint. Our fourth witness is Louis Saccoccio, chief executive officer of the national Health Care Anti-Fraud Association; fifth, Mr. Neville Pattinson, testifying on behalf of the Secure ID Coalition; sixth, Mr. Michael Terzich, senior vice president of global sales and marketing at Zebra Technologies. And, finally, we have Dr. Kevin Fu, associate professor of computer science and engineering at the University of Massachusetts, Amherst.

We are happy to have all of you here with us today. Your written testimony will be madea part of the record. We will ask that you summarize in 5 minutes verbally your testimony before beginning questions and answers from the committee.

Ms. King, you are recognized for 5 minutes.

**STATEMENTS OF KATHLEEN M. KING, DIRECTOR, HEALTH CARE, GOVERNMENT ACCOUNTABILITY OFFICE; DAN OLSON, DIRECTOR OF FRAUD PREVENTION, HEALTH INFORMATION DESIGNS, LLC; ALANNA M. LAVELLE, DIRECTOR, SPECIAL INVESTIGATIONS, WELLPOINT, INC.; LOUIS SACCOCCIO, CHIEF EXECUTIVE OFFICER, NATIONAL HEALTH CARE ANTI–FRAUD ASSOCIATION; NEVILLE PATTINSON, SENIOR VICE PRESIDENT, GEMALTO, INC., ON BEHALF OF THE SECURE ID COALITION; MICHAEL H. TERZICH, SENIOR VICE PRESIDENT, GLOBAL SALES AND MARKETING, ZEBRA TECHNOLOGIES CORP.; AND KEVIN FU, ASSOCIATE PROFESSOR IN COMPUTER SCIENCE AND ENGINEERING, UNIVERSITY OF MICHIGAN AND UNIVERSITY OF MASSACHUSETTS AMHERST**

## STATEMENT OF KATHLEEN M. KING

Ms. KING. Chairman Pitts, Ranking Member Pallone, and members of the subcommittee, I am pleased to be here today to discuss our work regarding Medicare fraud, including the types of providers involved in fraud and strategies we have identified that could help prevent or detect fraud.

Since 1990, we have designated Medicare as a high-risk program because its size and complexity make it vulnerable to fraud. Recently, for the first time, we were able to identify the types of providers investigated for and convicted of fraud, which should help CMS and other agencies target their efforts to prevent and reduce fraud.

In our work, we defined the subject of fraud cases as either institutions or individuals. We found that many different types of providers were investigated for fraud. In 2010, medical facilities, such as medical centers, clinics, and practices, were the most frequent subjects of criminal fraud investigations, accounting for about a quarter of all investigations, followed by durable medical equipment suppliers, which accounted for 16 percent. Beneficiaries accounted for 3 percent of investigations.

Of these, the HHS Office of Inspector General referred about 15 percent of the subjects investigated for criminal fraud to the Department of Justice for prosecution. And in 2010, nearly 1,100 subjects were charged in criminal fraud cases. Of those charged, approximately 85 percent were found guilty, pled guilty, or pled no contest. Medical facilities and DME suppliers accounted for about 40 percent of these subjects.

With respect to civil fraud cases, about 2,300 subjects were investigated in 2010. Hospitals and other medical facilities accounted for nearly 40 percent of the subjects in the civil cases that were pursued. According to the OIG, about 40 percent of the—I am sorry, about 50 percent of the cases were pursued, and the remaining cases were not pursued for a variety of reasons, including lack of resources and insufficient evidence.

Of the subjects pursued, about 60 percent resulted in judgments or settlements. And, again, hospitals and other medical facilities accounted for about 40 percent of the judgments. None of the subjects were beneficiaries.

Turning to strategies to reduce fraud, we have identified three, including strengthening provider enrollment processes and standards; improving pre- and post-payment review of claims; and developing processes to address identified vulnerabilities.

CMS has made progress in each of these areas through implementing provisions of the Affordable Care Act and the Small Business Jobs Act. For example, CMS now has a process in place to better screen providers before enrolling them in Medicare. And it has implemented the fraud prevention system, which detects suspicious claims before they are paid.

Still, further action is needed. We have made a number of recommendations to CMS that have not been implemented, and we continue to urge CMS to adopt them.

In addition, we have significant ongoing work designed to assist CMS in its fraud-prevention efforts. We are currently assessing the effectiveness of the prepayment edits CMS and its contractors use to ensure that Medicare claims are paid correctly the first time. We also have a study under way examining how Federal agencies are allocating funds from the Health Care Fraud and Abuse Control Program, as well as evaluating the effectiveness of those efforts. And we are also examining the effectiveness of CMS's fraud contractors, the Zone Program integrity contractors.

Preventing and reducing fraud requires constant vigilance, as a wide variety of providers are involved in fraud and those intent on committing fraud will always seek new opportunities to circumvent program safeguards. We urge CMS to continues its efforts.

And this concludes my prepared statement. Thank you.

Mr. PITTS. The Chair thanks the gentlelady.

[The prepared statement of Ms. King follows:]

United States Government Accountability Office

GAO

Testimony
Before the Subcommittee on Health,
Committee on Energy and Commerce,
House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EST
Wednesday, November 28, 2012

# HEALTH CARE FRAUD

## Types of Providers Involved in Medicare Cases, and CMS Efforts to Reduce Fraud

Statement of Kathleen M. King
Director, Health Care

GAO
Accountability * Integrity * Reliability

Chairman Pitts, Ranking Member Pallone, and Members of the Subcommittee:

I am pleased to be here today to discuss our work regarding health care fraud in Medicare and to discuss strategies that could help reduce fraud. Since 1990, GAO has designated Medicare as a high-risk program, as its complexity and susceptibility to payment errors from various causes, added to its size, have made it vulnerable to fraud.[1] Although there have been convictions for multimillion dollar schemes that defrauded the Medicare program, the extent of the problem is unknown as there are no reliable estimates of the magnitude of fraud in the health care industry. Fraud is difficult to detect because those involved are engaged in intentional deception. According to the Department of Health and Human Services' Office of Inspector General (HHS-OIG), common health care fraud schemes include providers or suppliers billing for services or supplies not provided or not medically necessary, purposely billing for a higher level of service than that provided, misreporting data to increase payments, paying kickbacks to providers for referring beneficiaries for specific services or to certain entities, or stealing providers' or beneficiaries' identities.

Since 1997, Congress has provided funds specifically for activities to address fraud, as well as waste and abuse, in Medicare and other federal health care programs. In fiscal year 2011, the federal government allocated at least $608 million in funding to investigate and prosecute

[1] In 1990, we began to report on government operations that we identified as "high risk" for serious weaknesses in areas that involve substantial resources and provide critical services to the public. Medicaid is among those programs we have identified as high-risk and Medicare has been included since 1990. See GAO, *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: February 2011). See also http://www.gao.gov/highrisk/risks/insurance/medicare_program.php. Medicare is the federally financed health insurance program for persons age 65 or over, certain individuals with disabilities, and individuals with end-stage renal disease. Medicare Parts A and B are known as Medicare fee-for-service (FFS). Medicare Part A covers hospital and other inpatient stays. Medicare Part B is optional, and covers hospital outpatient, physician, and other services. Medicare beneficiaries have the option of obtaining coverage for Medicare services from private health plans that participate in Medicare Advantage—Medicare's managed care program—also known as Part C. All Medicare beneficiaries may purchase coverage for outpatient prescription drugs under Part D, either as a stand-alone benefit or as part of a Medicare Advantage plan. Fraud involves an intentional act or representation to deceive with the knowledge that the action or representation could result in gain.

cases of alleged fraud in health care programs.[2] The Centers for Medicare and Medicaid Services (CMS)—an agency within HHS—oversees Medicare, Medicaid, and the Children's Health Insurance Program (CHIP). Along with its contractors, CMS works to reduce fraud. The HHS-OIG along with the Department of Justice (DOJ)—including its Criminal and Civil Divisions, the U.S. Attorney's Offices (USAOs) throughout the country, and the Federal Bureau of Investigation (FBI)—work together to investigate and prosecute cases of health care fraud.

My testimony today focuses on the types of providers that have been investigated for fraud and the outcomes of those investigations, and strategies that could be used to combat Medicare fraud. This statement is informed primarily by our September 2012 report on health care fraud and 8 years of prior work on fraud, waste, and abuse in health care programs.[3] A full list of the products that this testimony is based on is provided at the end of this statement.

These products were developed using a variety of methodologies, including analyses of fraud investigations and outcomes data obtained from federal agencies, review of public court records, examination of relevant policies and procedures, and interviews with agency officials.[4] The work on which these products were based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

[2] See Department of Health and Human Services and Department of Justice, *Health Care Fraud and Abuse Control Program Annual Report for Fiscal Year 2011*: February 2012. The program, which is under the joint direction of the Attorney General and the Secretary of the Department of Health and Human Services (HHS) is designed to coordinate federal, state, and local law enforcement activities with respect to health care fraud and abuse. Additional funds to combat health care fraud spent by HHS and the Department of Justice (DOJ) are not included in this figure.

[3] See GAO, *Health Care Fraud: Types of Providers Involved in Medicare, Medicaid, and the Children's Health Insurance Program Cases;* GAO-12-820 (Washington, D.C.: Sep. 7, 2012).

[4] The products listed at the end of this statement contain detailed informetion on the methodologies used in our work.

## Medical Facilities Were the Most Frequent Subjects of Criminal Investigations, and Hospitals Were the Most Frequent Subjects of Civil Investigations

In recently completed work, we found that medical facilities (such as medical centers, clinics, and practices) and durable medical equipment suppliers were the most frequent subjects of criminal fraud cases in Medicare, Medicaid, and CHIP in 2010.[5] Hospitals and medical facilities were the most frequent subjects of civil fraud cases, including cases that resulted in judgments or settlements.

### Medical Facilities and Durable Medical Equipment Suppliers Were the Most Frequent Subjects of Criminal Fraud Cases in 2010

According to 2010 data, about one-quarter of the 7,848 subjects investigated in criminal health care fraud cases were medical facilities or were affiliated with these facilities. Additionally, about 16 percent of subjects were durable medical equipment suppliers. Among the subjects investigated in criminal fraud cases, a small percentage (approximately 3 percent) were individuals who were beneficiaries of health care programs.

Most of the subjects investigated for criminal fraud in 2010 were not pursued—meaning that the HHS-OIG did not refer the subject's case to DOJ for prosecution. According to the 2010 data, 1,086 subjects were charged in criminal fraud cases and approximately 85 percent of them (925 subjects) were found guilty, pled guilty, or pled no contest to some or all of the criminal charges against them. Among those subjects that were found or pled guilty or no contest, the most frequent subjects were medical facilities (18.7 percent) or durable medical equipment suppliers (18.5 percent). See table 1 below for additional information on subjects who were found or pled guilty or no contest in 2010 criminal cases by provider type.

[5] GAO-12-820. We use the term "subjects" to refer to individuals and entities involved in fraud cases. These subjects can be individuals, such as a dentist or a nurse; an organization, such as a pharmaceutical manufacturer; or a facility, such as a hospital.

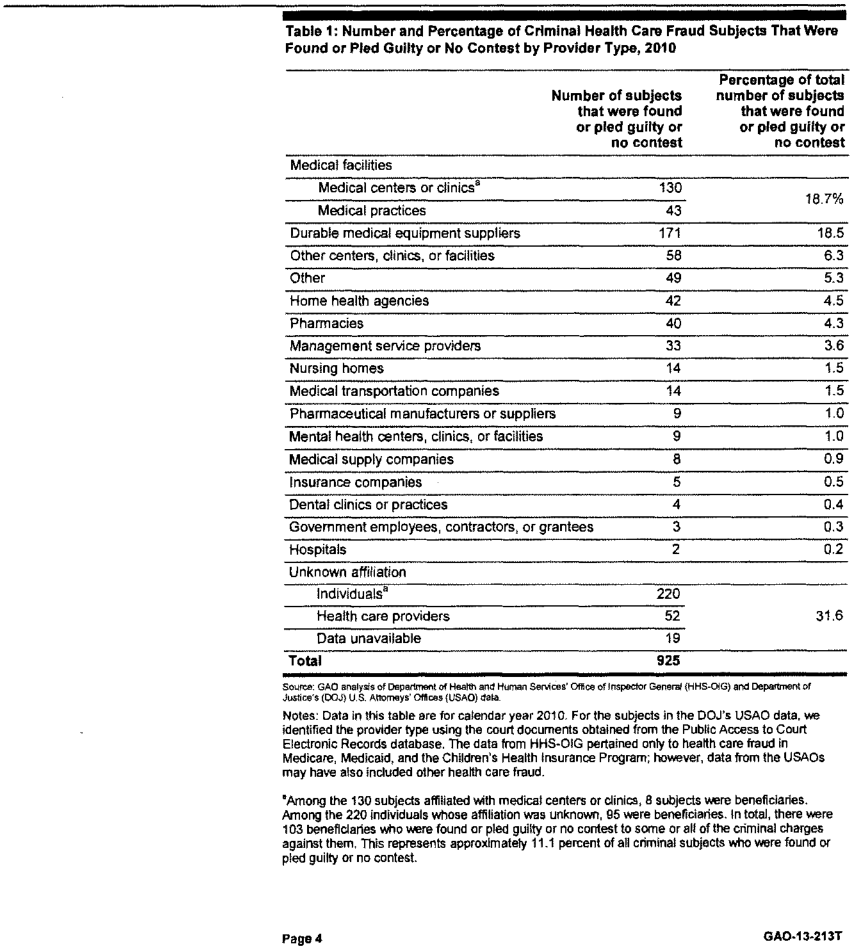


**Table 1: Number and Percentage of Criminal Health Care Fraud Subjects That Were Found or Pled Guilty or No Contest by Provider Type, 2010**

| | Number of subjects that were found or pled guilty or no contest | Percentage of total number of subjects that were found or pled guilty or no contest |
|---|---|---|
| Medical facilities | | |
| Medical centers or clinics[a] | 130 | 18.7% |
| Medical practices | 43 | |
| Durable medical equipment suppliers | 171 | 18.5 |
| Other centers, clinics, or facilities | 58 | 6.3 |
| Other | 49 | 5.3 |
| Home health agencies | 42 | 4.5 |
| Pharmacies | 40 | 4.3 |
| Management service providers | 33 | 3.6 |
| Nursing homes | 14 | 1.5 |
| Medical transportation companies | 14 | 1.5 |
| Pharmaceutical manufacturers or suppliers | 9 | 1.0 |
| Mental health centers, clinics, or facilities | 9 | 1.0 |
| Medical supply companies | 8 | 0.9 |
| Insurance companies | 5 | 0.5 |
| Dental clinics or practices | 4 | 0.4 |
| Government employees, contractors, or grantees | 3 | 0.3 |
| Hospitals | 2 | 0.2 |
| Unknown affiliation | | |
| Individuals[a] | 220 | 31.6 |
| Health care providers | 52 | |
| Data unavailable | 19 | |
| **Total** | **925** | |

Source: GAO analysis of Department of Health and Human Services' Office of Inspector General (HHS-OIG) and Department of Justice's (DOJ) U.S. Attorneys' Offices (USAO) data.

Notes: Data in this table are for calendar year 2010. For the subjects in the DOJ's USAO data, we identified the provider type using the court documents obtained from the Public Access to Court Electronic Records database. The data from HHS-OIG pertained only to health care fraud in Medicare, Medicaid, and the Children's Health Insurance Program; however, data from the USAOs may have also included other health care fraud.

[a] Among the 130 subjects affiliated with medical centers or clinics, 8 subjects were beneficiaries. Among the 220 individuals whose affiliation was unknown, 95 were beneficiaries. In total, there were 103 beneficiaries who were found or pled guilty or no contest to some or all of the criminal charges against them. This represents approximately 11.1 percent of all criminal subjects who were found or pled guilty or no contest.

Additionally, about 11 percent of the subjects found guilty or who pled guilty or no contest were beneficiaries of health care programs. Among the 925 subjects that were found or pled guilty or no contest, 103 subjects were beneficiaries—95 of whom are listed as individuals in Table 1 and 8 of whom were affiliated with medical centers or clinics. For example, in one of these criminal cases, a number of people associated with a medical clinic, including owners, an administrator, employees, a physician, and beneficiaries pled guilty or were convicted for their participation in a scheme to defraud Medicare. The fraud scheme involved recruiting beneficiaries through kickbacks for the purpose of submitting bills for injection and infusion treatments, which were not provided or not medically necessary.

## Hospitals and Medical Facilities Were the Most Frequent Subjects of Civil Fraud Cases, Including Cases That Resulted in Judgments or Settlements

Hospitals constituted nearly 20 percent of the 2,339 subjects of civil fraud cases investigated in 2010, and other medical facilities accounted for about 18 percent of the subjects. Less than 1 percent of subjects involved in civil health care fraud cases were beneficiaries of health care programs.

Not all of the subjects investigated in 2010 civil cases were pursued; by pursued, we mean that the USAO or DOJ's Civil Division received the case and took some sort of action. Approximately 47 percent of subjects were involved in civil cases that were pursued and the remaining 53 percent were involved in cases that were not pursued for a variety of reasons, including lack of resources or insufficient evidence as reported by the HHS-OIG. According to the 2010 data, 1,087 subjects were involved in civil fraud cases that were pursued, and among those, 602 subjects were involved in cases that resulted in a judgment or settlement for the government or the relator.[6] Twenty-seven percent of the subjects in cases that were pursued were hospitals, and about 17 percent were medical facilities. None of those 602 subjects were beneficiaries of health care programs. See table 2 for additional information on provider types for

[6] Individuals, known as relators, can bring civil health care fraud suits in the name of the government under the False Claims Act (FCA). The FCA prohibits certain actions, including the knowing presentation of a false claim for payment by the federal government. 31 U.S.C. § 3729(a)(1)(A). In these cases, known as qui tam cases, the relator can receive a portion of a monetary settlement, and reasonable expenses and attorneys' fees and costs. 31 U.S.C. § 3730(b),(d).

subjects where the case resulted in a settlement or judgment for the government or relator.

**Table 2: Number and Percentage of Subjects in Civil Health Care Fraud Cases with Judgment for Government or Relator, Settlement, or Both by Provider Type, 2010**

| | Number of subjects with judgment, settlement, or both | Percentage of total number of subjects with judgment, settlement, or both |
|---|---|---|
| Hospitals | 165 | 27.4% |
| Medical facilities | | |
| Medical practices | 65 | |
| Medical centers or clinics | 35 | 16.6 |
| Other centers, clinics, or facilities | 41 | 6.8 |
| Home health agencies | 34 | 5.6 |
| Nursing homes | 26 | 4.3 |
| Durable medical equipment suppliers | 25 | 4.2 |
| Management service providers | 21 | 3.5 |
| Dental clinics or practices | 21 | 3.5 |
| Pharmaceutical manufacturers or suppliers | 19 | 3.2 |
| Insurance companies | 15 | 2.5 |
| Pharmacies | 13 | 2.2 |
| Medical transportation companies | 11 | 1.8 |
| Mental health centers, clinics, or facilities | 5 | 0.8 |
| Other | 5 | 0.8 |
| Medical supply companies | 3 | 0.5 |
| Government employees, contractors, or grantees | 2 | 0.3 |
| Unknown affiliation | | |
| Data unavailable | 58 | |
| Health care providers | 34 | |
| Individuals | 4 | 15.9 |
| **Total** | **602** | |

Source: GAO analysis of Department of Health and Human Services Office of the Inspector General (HHS-OIG), Department of Justice's U.S. Attorneys' Offices (USAOs), and DOJ's Civil Division data.

Notes: Data in this table are for calendar year 2010. For the subjects in the USAOs and DOJ's Civil Division data, we identified the provider type using the court documents obtained from the Public Access to Court Electronic Records database. The data from HHS-OIG pertained only to health care fraud in Medicare, Medicaid, and the Children's Health Insurance Program; however, data from the USAOs and DOJ's Civil Division may also include other health care fraud.

## CMS Has Made Progress in Implementing Strategies to Prevent Fraud, but Further Actions are Needed

CMS has made progress in implementing strategies to prevent fraud, and recent legislation provided it with enhanced authority. However, CMS has not implemented some of the key strategies we identified in our prior work to help CMS address challenges it faces in preventing fraud. Among others, these strategies include strengthening provider enrollment processes and standards, improving pre- and post-payment claims review, and developing a robust process for addressing identified vulnerabilities.

- **Strengthening provider enrollment processes and standards**—As we have reported in the past, strengthening the standards and procedures for provider enrollment could help reduce the risk of enrolling providers intent on defrauding Medicare.[7] Although CMS has taken some important steps to identify and prevent fraud, including implementing provisions in Patient Protection and Affordable Care Act (PPACA), such as screening providers by risk level, more remains to be done to prevent making erroneous Medicare payments because of fraud.[8] In particular, we have found CMS could do more to strengthen provider enrollment screening to avoid those intent on committing fraud, such as requiring a surety bond for certain types of at-risk providers and additional disclosure of information such as previous payment suspensions from other federal programs.

- **Improving pre- and postpayment review of claims**—As we have reported in the past, having robust controls in claims payment systems to prevent payment of problematic claims can help reduce loss.[9] Effective prepayment edits that deny claims for ineligible providers and suppliers depends on having timely and accurate information about them, such as whether the providers are currently enrolled and have the appropriate license or accreditation to provide specific services. In prior work, we found weaknesses in the database that maintains Medicare provider and supplier enrollment information related to the frequency with which CMS's contractors update

[7] See GAO, *Medicare Program Integrity: CMS Continues Efforts to Strengthen the Screening of Providers and Suppliers,* GAO-12-351, (Washington, D.C.: Apr. 10, 2012).

[8] Pub. L. No. 111-148, 124 Stat.119 (2010), as amended by Health Care and Education Reconciliation Act of 2010 (HCERA), Pub. L. No. 111-152, 124 Stat. 1029, which we refer to collectively as PPACA.

[9] See GAO, *Medicare: Progress Made to Deter Fraud, but More Could Be Done,* GAO-12-801T, (Washington, D.C.: June 8, 2012).

enrollment information and the timeliness and accuracy of information.[10] Although CMS is working to improve the timeliness and accuracy of the provider and supplier information, it is too soon to tell if these efforts will better prevent payments to ineligible providers and suppliers. Additionally, further actions are needed to improve use of CMS technology systems that could help CMS and program integrity contractors identify fraud both before and after claims have been paid.[11] For example, we recently examined CMS's new predictive analytics system—the Fraud Prevention System—and found that although it has been implemented and is in use, it is not yet fully integrated with existing information technology systems. This level of integration would allow for the prevention of payments until suspect claims can be investigated and determined to be valid.[12] To ensure that the implementation of the Fraud Prevention System is successful, we recommended to CMS that it define quantifiable benefits expected and mechanisms for measuring the results of using the system. In response to our report, HHS officials agreed with our recommendation and noted that CMS intends to establish outcome-based performance targets based on the first year of the system's implementation.

- **Developing a robust process for addressing identified vulnerabilities**—As we have reported in the past, having mechanisms in place to resolve vulnerabilities that lead to improper payments is critical to effective program management and could help address fraud.[13] For example, fraud in the Medicare program can be reduced by making it more difficult for thieves to steal beneficiaries' Social Security numbers (SSN), which are printed on beneficiaries' Medicare cards. In recent work, we found that CMS had not committed to a plan for removing SSNs from Medicare cards, and that CMS's cost estimates for options it explored to remove SSNs were not well documented or reliable. We recommended that CMS select an approach for removing the SSN from the Medicare card that best

[10] GAO-12-351.

[11] See GAO, *Fraud Detection Systems: Centers for Medicare and Medicaid Services Needs to Ensure More Widespread Use*, GAO-11-475 (Washington, D.C.: June 30, 2011).

[12] See GAO, *Medicare Fraud Prevention: CMS Has Implemented a Predictive Analytics System, but Needs to Define Measures to Determine Its Effectiveness*, GAO-13-104 (Washington, D.C.: Oct. 15, 2012).

[13] GAO-12-801T.

protects beneficiaries from identity theft and minimizes burdens for providers, beneficiaries, and CMS; we also recommended that CMS develop an accurate, well-documented cost estimate for such an option using standard cost-estimating procedures.[14] CMS agreed with our recommendation and indicated that it would take steps to revise its cost estimates on the basis of concerns we highlighted.

Although CMS has taken some important steps to identify and prevent fraud, including implementing provisions in PPACA, more remains to be done to prevent making erroneous Medicare payments because of fraud. It is critical that CMS implement and make full use of new authorities granted by recent legislation, as well as incorporate recommendations made by us, and the HHS-OIG in these areas. Moving from "pay and chase" to effective deterrence that prevents fraud from occurring in the first place is key to ensuring that federal funds are used efficiently and for their intended purposes.

As the authorities and requirements in recent legislation become part of Medicare's operations, additional evaluation and oversight will be necessary to determine whether they are implemented as required and have the desired effect. We are investing significant resources in a body of work that assesses CMS efforts to refine and improve its fraud detection and prevention efforts. Notably, we are assessing the effectiveness of different types of prepayment edits in Medicare and of CMS's oversight of its contractors in implementing those edits to help ensure that Medicare pays claims correctly the first time. Additionally, we have a study underway that is examining how federal agencies—such as CMS, HHS-OIG, and DOJ—are allocating funds received from the Health Care Fraud and Abuse Control Program to reduce fraud, as well as the effectiveness of such efforts. We are also examining a number of issues concerning CMS's oversight and management of its Zone Program Integrity Contractors—the contractors responsible for detecting and investigating potential fraud—including how they prioritize their work and are evaluated by CMS. In addition, we are examining CMS's oversight of some of the contractors that conduct reviews of claims after payment. These studies are focused on additional actions for CMS that could help the agency more systematically reduce fraud in the Medicare program.

[14] See GAO, *Medicare: CMS Needs an Approach and a Reliable Cost Estimate for Removing Social Security Numbers from Medicare Cards*, GAO-12-831 (Washington, D.C.: Aug. 1, 2012).

Because of the amount of program funding at risk, fraud will remain an inherent threat to Medicare, so continuing vigilance to reduce vulnerabilities will be necessary. Individuals intent on defrauding Medicare will continue to develop new approaches to try to circumvent program safeguards and investigative and enforcement efforts. Although targeting certain types of providers that CMS has identified as high risk may be useful, it may allow other types of providers committing fraud to go unnoticed. We will continue to assess efforts to fight fraud and provide recommendations to CMS, as appropriate, that we believe will assist the agency and its contractors in this important task. We urge CMS to continue its efforts as well.

Chairman Pitts, Ranking Member Pallone, and Members of the Subcommittee, this concludes my prepared statement. I would be happy to answer any questions you or other members of the subcommittee may have.

If you or your staff have any questions about this testimony, please contact me at (202) 512-7114 or kingk@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Martin T. Gahart, Assistant Director; Christie Enders; and Drew Long were key contributors to this statement.

# Related GAO Products

*Medicare Fraud Prevention: CMS Has Implemented a Predictive Analytics System, but Needs to Define Measures to Determine Its Effectiveness.* GAO-13-104. Washington, D.C.: October 15, 2012.

*Health Care Fraud: Types of Providers Involved in Medicare, Medicaid, and the Children's Health Insurance Program Cases.* GAO-12-820. Washington, D.C.: September 7, 2012.

*Medicare: CMS Needs an Approach and a Reliable Cost Estimate for Removing Social Security Numbers from Medicare Cards.* GAO-12-831. Washington, D.C.: August 1, 2012.

*Medicare: Progress Made to Deter Fraud, but More Could Be Done.* GAO-12-801T. Washington, D.C.: June 8, 2012.

*Medicare Program Integrity: CMS Continues Efforts to Strengthen the Screening of Providers and Suppliers.* GAO-12-351. Washington, D.C.: April 10, 2012.

*Improper Payments: Remaining Challenges and Strategies for Governmentwide Reduction Efforts.* GAO-12-573T. Washington, D.C.: March 28, 2012.

*2012 Annual Report: Opportunities to Reduce Duplication, Overlap and Fragmentation, Achieve Savings, and Enhance Revenue.* GAO-12-342SP. Washington, D.C.: February 28, 2012.

*Fraud Detection Systems: Centers for Medicare and Medicaid Services Needs to Expand Efforts to Support Program Integrity Initiatives.* GAO-12-292T. Washington, D.C.: December 7, 2011.

*Medicare Part D: Instances of Questionable Access to Prescription Drugs.* GAO-12-104T. Washington, D.C.: October 4, 2011.

*Medicare Part D: Instances of Questionable Access to Prescription Drugs.* GAO-11-699. Washington, D.C.: September 6, 2011.

*Medicare Integrity Program: CMS Used Increased Funding for New Activities but Could Improve Measurement of Program Effectiveness.* GAO-11-592. Washington, D.C.: July 29, 2011.

*Improper Payments: Reported Medicare Estimates and Key Remediation Strategies.* GAO-11-842T. Washington, D.C.: July 28, 2011.

*Fraud Detection Systems: Additional Actions Needed to Support Program Integrity Efforts at Centers for Medicare and Medicaid Services.* GAO-11-822T. Washington, D.C.: July 12, 2011.

*Fraud Detection Systems: Centers for Medicare and Medicaid Services Needs to Ensure More Widespread Use.* GAO-11-475. Washington, D.C.: June 30, 2011.

*High-Risk Series: An Update.* GAO-11-278. Washington, D.C.: February 16, 2011.

## GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

### Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

## Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov.

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

## Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

## Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Please Print on Recycled Paper.

Mr. PITTS. Mr. Olson, you are recognized for 5 minutes for an opening statement.

## STATEMENT OF DAN OLSON

Mr. OLSON. Thank you. Good morning, Chairman Pitts, Ranking Member Pallone, and congressional leaders. Thank you so much for the opportunity to testify on the issue of examining options to combat healthcare fraud, waste, and abuse within the Medicare and Medicaid programs.

I am Dan Olson. I am the director of fraud prevention for Health Information Designs, which is a national healthcare analytics company. I oversee our product offering for fraud called SURVEIL, and I have worked in the program integrity field for over 17 years.

Thank you for entering my full comments, as I will summarize today my testimony.

Today we recognize that healthcare fraud is indeed a criminal problem. It is multidimensional and has many facets to it. But I suggest to you today and recommend that we need a multidimensional toolset to address healthcare fraud, waste, and abuse. Within this toolset we need to have something that is dynamic in nature, nimble to change, and responsive to emerging trends.

Several items that I would suggest this morning are: the traditional business rules, which has been in place for a long time, which evaluates medical guidelines and Federal and State policy. But to enhance this, we must have predictive models, which are using past claims and billing behaviors to forecast future actions. We must also include predictive analytics, which is developing statistical models to identify unknown data relationships. We must include link analysis, which identify relationships between providers, billing entities, and recipients, often where we can find kickbacks so they don't become so prevalent. We must also incorporate clinical decision support systems so that we no longer look at just volume-based metrics but we look at clinical guidelines to identify areas where patients are at risk for developing major medical issues.

I must caution, though, against the belief that the toolkit can stand alone because simply it cannot. The toolkit must be managed by a broad-based partnership that includes medical professionals, includes legal entities, analytical professionals, investigative entities, coding experts, statisticians, et cetera. By so doing that, we will have a toolkit that can address the multi facets of fraud, waste, and abuse.

As has been mentioned, significant progress has already been made in the healthcare world, but significant progress needs to continue to be made. Healthcare fraud is dynamic; it is not static. If we sit and do nothing or rely on what we have done in the past, we will be behind the curve. We must implement the following recommendations that I present this morning.

First, we should continue to expand the Medicare Fraud strike force at the Federal level, but not only that, we must implement it at the State level. By implementing it at the State level—and I would recommend that each of the regional CMS offices oversee this—then we can improve upon and recover greater than 1 percent of the overall Medicare and Medicaid spend.

We must continue and I recommend to expand and fund the Integrated Data Repository. The singular importance of this alone can simply not be overstated. I recommend that CMS adopt a regionalized approach to this implementation that will allow for a more rapid development and will reduce the testing and training time that is needed for deployment. It is estimated that over $250 million can be accomplished in recoveries during the initial year and over $100 million in successive years.

We must also continue to expand the do-not-pay list that was originally implemented by including retired and sanctioned Drug Enforcement Agency numbers. Estimated savings: $200 million.

Finally, we must also publish national and statewide healthcare statistics. We have read time and again about something called a national healthcare fraud hotspot, where we see billings in excess of 3,000 percent or 2,000 percent. These are absurd. We need to know this. This needs to be in front of us so that we can act upon it.

In order to do this, I recommend that we establish baseline thresholds at the provider level for Medicare and Medicaid; that these threshold lists be updated regularly; and that they be published on the CMS Web site so that fraud analysts can further act on them and know what emerging trends and patterns will be.

I would be happy to expand on any of these issues that I presented this morning. I have also included these in much more detail in the two white papers that are attached as appendices to my testimony.

I would like to thank you, Congressman Pitts, Ranking Member Pallone, and congressional leaders, for this opportunity to present. And I look forward to the question-and-answer time that will follow. Thank you.

Mr. PITTS. The Chair thanks the gentleman.

[The prepared statement of Mr. Olson follows:]

# STATEMENT OF

DAN OLSON, CFE

DIRECTOR OF FRAUD PREVENTION

HEALTH INFORMATION DESIGNS, LLC

ON

# EXAMINING OPTIONS TO COMBAT HEALTH CARE WASTE, FRAUD, AND ABUSE

BEFORE THE

UNITED STATES ENERGY AND COMMERCE COMMITTEE

SUBCOMMITTEE ON HEALTH

NOVEMBER 28, 2012

HEALTH
INFORMATION
DESIGNS

SURVEIL

# U.S. Energy and Commerce Committee
# Subcommittee on Health

## Hearing on Examining Options to Combat Health Care Waste, Fraud, and Abuse

## November 28, 2012

Good morning Chairman Pitts, Ranking Member Pallone, and Congressional leaders. Thank you for the invitation to testify about Examining Options to Combat Health Care Waste, Fraud, and Abuse in the Medicare and Medicaid programs. I am the Director of Fraud Prevention at Health Information Designs, a national health care analytics company. I oversee our fraud and abuse detection product offering, SURVEIL®, and have worked in the program integrity field for over 17 years.

### Introduction

The General Accounting Office estimates that over $70 billion dollars each year are lost to health care fraud, waste, and abuse. During FY 2011, over $4 billion dollars were recovered. This amount represents the single largest health care fraud recovery in history[i], but is still less than 1% of the overall spending for the Medicare and Medicaid programs.

Health care fraud is a criminal problem. The deceptive nature of fraud expands through complex relationships and multiple layers of individuals and entities that seek to protect the criminal element. Often, the conduit of the abuse remains two or more steps removed from the perpetrator. Fraud remains a difficult, troubling issue, which requires sophisticated solutions.

### A New Tool Kit

I am here this morning to present additional options to combat health care fraud and abuse—by expanding the traditional health care fraud toolkit. Due to the dynamic nature of health care fraud, our toolkit cannot be one or even two-dimensional. Even the most sophisticated tools, if left static, will become obsolete as fraudsters work around them. Like fraud itself, our toolkit must incorporate tools that are dynamic in nature, nimble to change, and responsive to emerging patterns.

The tools to be considered for inclusion in our toolkit can include the following:

- Traditional business rules – incorporating claim edits based on medical guidelines or federal and state policy.
- Predictive models – using past claim or billing behavior to forecast future actions.
- Predictive analytics – developing statistical models to identify unknown data relationships.
- Link analysis – data analysis technique to identify relationships between providers, recipients, and billing entities.
- Clinical decision support systems – using claims data to determine which patients are at risk of developing major medical conditions.

We must caution against the belief that the toolkit can stand alone. The toolkit must be managed by a broad-based partnership that includes data analysts, investigators, auditors, medical consultants, statisticians, programmers, certified coders, law enforcement, policy experts, and attorneys.

## Expand Current Efforts

We have made significant progress to combat health care fraud, waste and abuse. The following areas can be expanded to generate additional savings for the Medicare and Medicaid programs.

- **Expand the Medicare Fraud Strike Force at the federal level and enact it at the State level.** The Medicare Fraud Strike Force has experienced groundbreaking success during the past year. Expansion of the Strike Force model to the state level with oversight by each regional CMS office will expand the current 1% recovery of federal and state dollars lost to health care fraud.

- **Continue to fund and expand the Integrated Data Repository.** The goal of the Integrated Data Repository (IDR) is to create a database that contains multiple years of Medicare and Medicaid data. In July 2011, the General Account Office (GAO) issued a report entitled *Fraud Detection Systems: Additional Actions Needed to Support Program Integrity Efforts at Centers for Medicare and Medicaid Services.*[ii] The report showed that the IDR has been only partially rolled out and that Medicaid data has not been incorporated into the system. Complete system implementation is pending additional software development at the federal level and funding for states to provide their data to CMS. I recommend that CMS adopt a regionalized approach to development that will allow for more rapid development and shortened testing and training cycles. Expansion of the IDR could generate $250M or more during initial implementation and more than $100M in subsequent years.

- **Expand the "Do Not Pay" list to include retired or sanctioned Drug Enforcement Agency (DEA) numbers.** On June 18, 2010, a presidential memorandum was issued entitled *Enhancing Payment Accuracy Through a "Do Not Pay List."* The memorandum ordered the creation of a centralized database that federal agencies will be required to search before distributing payments to contractors and providers. Currently, the "Do Not Pay List" does not include a cross-match of the data in the Medicare/Medicaid claim and DEA registry. I recommend that validation of the DEA numbers occur prior to payment. This recommendation could generate savings of $200M or more during initial implementation and up to $100M in subsequent years.

- **Calculate and publish national and state-wide health care statistics.** The DOJ, FBI, and OIG are using advanced data analysis techniques to evaluate health care claims. These techniques include identifying high-billing levels in health care fraud "hot spots," so that analysts can target emerging fraud schemes. I recommend that access to the national fraud hot spots be published so that health care fraud data analysts can gain insights into national standards and determine if potential abuses are occurring. I further recommend that the following steps be taken to provide health care fraud data analysts with additional information to uncover emerging schemes.
  - Establish baseline thresholds by provider type at the Medicare and Medicaid level
  - Update the threshold list at least quarterly
  - Publish the threshold list on the CMS website

This recommendation holds promise to increase critical resources essential to health care data analysis, identify emerging health care schemes, and generate additional savings for the Medicare and Medicaid programs.

I would be happy to expand on any of the above items during our question and answer time.

## Conclusion

Thank you, Chairman Pitts, Ranking Member Pallone, and Congressional leaders for this opportunity to present. I have written two white papers that address this subject in more detail and have provided these as appendices to my written testimony. At this time, I will be happy to answer any questions.

[i.] http://www.justice.gov/iso/opa/ag/speeches/2012/ag-speech-120214.html

[ii.] http://www.gao.gov/new.items/d11822t.pdf

# Tackling Fraud, Waste, and Abuse in the Medicare and Medicaid Programs:

*Response to the May 2 Open Letter to the Healthcare Community*

**Dan Olson, CFE**

June 2012

HEALTH
INFORMATION
DESIGNS

# Contents

***On May 2, 2012, the Senate Finance Committee issued a letter to the healthcare sector soliciting industry stakeholder insights on ways to combat fraud, waste, and abuse in the Medicare and Medicaid programs. The letter followed an April 25th hearing about the effectiveness of fraud-fighting efforts at which members of the committee questioned government officials from the OIG, CMS, and GAO. The letter invited recommendations from the public and private sectors for program integrity reforms that would strengthen current efforts to prevent unlawful conduct and waste involving government healthcare programs. This White Paper is a direct response to that invitation.***

# I. Introduction

The past four years offer examples of unprecedented partnering efforts that have served the common good by tackling healthcare fraud and abuse issues in the federal and state Medicare and Medicaid programs. The Department of Health and Human Services (HHS) and the Department of Justice (DOJ) have been at the forefront of these efforts. Early successes from their partnership have raised the hope of additional multi-million dollar fraud takedowns resulting from increased vigilance, sophisticated new technology, and harsher punishment of felons. It is well-documented that the HHS/DOJ partnership resulted in the largest annual healthcare fraud recovery in history during FY 2011—over $4 billion dollars.[1] This dollar amount recovery demonstrates a 58% increase over the amount recovered in FY 2009. Other statistics are impressive as well: the number of new healthcare fraud cases opened in 2011 shows a 43% increase from the previous year. On the state side, program integrity assessment records show that states collected over $2.3 billion in FY 2009.[2]

Despite these initial successes, we must be circumspect in feeling that a simple continuation of current initiatives will fully address Medicare and Medicaid healthcare fraud. The dollar recovery amounts for Medicare and Medicaid (using 2011 and 2009 data respectively) represent less than 1% of their overall spending. The fact remains that healthcare fraud is first and foremost a criminal problem. The deceptive nature of fraud expands through complex relationships and multiple layers of individuals and entities that seek to protect the criminal element. Hidden within these relationships are patterns and trends that reveal the true identity of the perpetrator(s) and the nature of their criminal act. Often, the conduit of the abuse remains two or more steps removed from the perpetrator. These are difficult and troubling issues.

In May 2012, six members of the Senate Finance Committee published an open letter to members of the healthcare community. In the letter, the lawmakers invited interested stakeholders to submit white papers offering recommendations and innovative solutions to improve program integrity efforts, strengthen payment reforms, and enhance fraud and abuse prevention efforts.

New initiatives are crucial, but it is also important to leverage momentum from existing successes. This White Paper offers recommendations for both new and enhanced policies and legislation to address and prevent healthcare fraud and abuse, focusing on the following specific areas:

- Program Integrity Reforms to Protect Beneficiaries and Prevent Fraud and Abuse
- Payment Integrity Reforms to Ensure Accuracy, Efficiency, and Value

| Recommendation Summary | | |
|---|---|---|
| Recommendation | Potential 1st Year Savings* / Benefit | Potential Yearly Subsequent Savings* / Benefit |
| Expand Medicare Fraud Strike Force Model | Increased federal and state fraud recoveries | Increased federal and state fraud recoveries |
| Expand Integrated Data Repository | $250M | $100M |
| Expand "Do Not Pay List" | $200M | $100M |
| Publicize Drug Expiration Dates | $100M | $50M |
| Match Vital Records to SSA and State MMIS | $100M | $50M |
| Require Provider Re-enrollment | Cost avoidance | Cost avoidance |
| Publish National and State Healthcare Statistics | Improved resources to fight fraud and abuse | Improved resources to fight fraud and abuse |
| Establish Central Repository of Fraud and Abuse Cases | Improved education | Improved education |

*Potential savings amounts are derived from historical reports showing dollars that were lost due to similar circumstances.

# II. Recommendations

This White Paper offers eight recommendations to improve federal and state efforts in combating waste, fraud, and abuse in the Medicare and Medicaid programs. The recommendations focus on expanding existing efforts through cooperation between Medicare and Medicaid and increasing data sharing by removing data silos.

All recommendations in this White Paper are predicated on the following objectives:

- Protection of Medicare and Medicaid recipients' privacy in accordance with the Health Insurance Portability and Accountability Act (HIPAA)
- Delivery of high quality services by Medicare and Medicaid providers
- Stewardship of taxpayer monies that fund the Medicare and Medicaid programs

## Recommendation 1 – Expand the Medicare Fraud Strike Force Model

***Create a Medicaid Fraud Strike Force at the state level***

Efforts to combat healthcare fraud and abuse have moved beyond the evaluation of low hanging fruit. Sophisticated criminals increasingly use multi-layered conspiracies to evade detection by healthcare fraud data analysts. New fraud techniques include money laundering using shell companies, organized crime, drug diversion, tax evasion, and kickback schemes. One such example occurred on March 29, 2012 when a doctor and his mother were indicted for a $1.2 million scheme involving drug distribution and tax crimes.[3]

The Medicare Fraud Strike Force has experienced groundbreaking success during the past ten months. Key to this success are the unprecedented partnering efforts among the HHS, Office of Inspector General (OIG), Federal Bureau of Investigation (FBI), and Internal Revenue Service (IRS); and the employment of enhanced data analytics technology. The following four examples illustrate the power of these partnering efforts in terms of monetary recoupments to federal programs:

- $295M – On September 7, 2011, 91 individuals were charged for submitting false claims.[4]
- $225M – On February 17, 2012, 111 individuals were charged for submitting false claims.[5]
- $375M – On February 28, 2012, one physician and his accomplices were charged for submitting false claims.[6]
- $452M – On May 16, 2012, 107 individuals were charged for submitting false claims.[7]

This White Paper recommends that the Medicare Fraud Strike Force continue to be expanded at the federal level and be enacted at the state Medicaid level. Recommendations for the state model include:

- Collective membership: State Medicaid Agency, Medicaid Fraud Control Unit, Attorney General, District Attorney, FBI, DEA, IRS, Professional Regulations, Vital Records, and contractual subject matter experts

- Requirement to execute Data Sharing Agreements among all task force entities
- Requirement to meet at least bi-monthly
- Requirement to produce an annual report of state task force activity
- Federal Financial Participation matches to support any pilot project undertaken by the task force
- Oversight by regional CMS office
- Repository to store all task force annual reports, established and maintained by CMS

Leveraging the power of the existing Medicare Fraud Strike Force and combining this with state-level Medicaid Fraud Strike Forces could create a synergy with the potential to bring about unparalleled success in fighting fraud and abuse.

### Potential Savings

Recommendation 1 holds promise for increasing yearly healthcare fraud recoveries well beyond the amount (less than 1%) that is currently being recovered.

## Recommendation 2 – Expand Integrated Data Repository

***Continue to fund and expand Integrated Data Repository***

The singular importance of the continued development and implementation of the Integrated Data Repository (IDR) cannot be overstated. The IDR and the One Program Integrity (One PI) Web portal—with its suite of analytic tools—have the potential to reinvent the manner in which healthcare data analytics are utilized. Breaking down existing data silos and moving data into a seamless integrated system will advance the cause of healthcare fraud prevention and elevate the analysis of Medicare and Medicaid claims data to a new level.

In July 2011, the General Account Office (GAO) issued a report entitled *Fraud Detection Systems: Additional Actions Needed to Support Program Integrity Efforts at Centers for Medicare and Medicaid Services.*[8] The report showed that the IDR has been only partially rolled out and that Medicaid data has not been incorporated into the system. Complete system implementation is pending additional software development at the federal level, and funding for states to provide their data to CMS.

In the interim, this White Paper recommends the following:

- Develop regionalized IDRs consistent with the ten CMS regions. Aligning the IDRs consistently with the existing CMS regions will take advantage of the existing infrastructure and minimize the disruption that a new initiative creates.
- Maintain the data protocols developed for the federal IDR and mirror them in each regional IDR.
- Restrict the initial data load (for example, one year) until testing is complete.
- Roll out claims by provider type to ensure the system is functioning properly. For example, the initial data load should only include physician data.
- Restrict the initial roll-out to a minimum data set.
- Conduct testing and training of each database with a cross-section of federal, state, and contractual subject matter experts.

A regionalized approach to development will allow for more rapid development and shortened testing and training cycles, thereby maximizing the benefits obtained at the Medicare and Medicaid levels.

### Potential Savings

Recommendation 2 holds promise for generating $250M or more during initial implementation and more than $100M in subsequent years. The savings estimate is based on first year savings generated from other Affordable Care Act initiatives. It is expected that once these changes are implemented, savings will increase beyond these projections as a result of richer data stores available to healthcare fraud data analysts.

## Recommendation 3 – Expand "Do Not Pay List"

### *Expand "Do Not Pay List" to include retired or sanctioned Drug Enforcement Agency (DEA) numbers*

On June 18, 2010, a presidential memorandum was issued entitled *Enhancing Payment Accuracy Through a "Do Not Pay List."* The memorandum ordered the creation of a centralized database that federal agencies will be required to search before distributing payments to contractors and providers. The "Do Not Pay List" was prompted by a three-year report from federal auditors that revealed that federal agencies paid $180 million in benefits to 20,000 deceased individuals and over $230 million to about 14,000 fugitives or incarcerated felons who are ineligible for benefits.[9]

The Department of Justice, Office of Drug Diversion maintains a file of all practitioners who have been assigned a DEA number. The file is updated monthly with new DEA registrants, reinstated DEA numbers, and retired DEA numbers. Fields include:

- DEA number
- Provider name, ID, and address
- Date of original registration
- Expiration date
- Drug schedules
- State license number
- State controlled substance number

The following data integrity benefits will be achieved by performing a cross-match of the data in Medicare/Medicaid claims and DEA registry:

- Validation of the DEA number submitted on the claim
- Confirmation that the DEA number is active on the DEA registry prior to paying the claim
- Confirmation that the DEA registrant has permission to dispense prescriptions in the state of origin on the claim
- Identification of the prescriber for those instances where the prescriber is not enrolled by Medicare or Medicaid

### Potential Savings

Recommendation 3 holds promise for generating $200M or more during initial implementation and up to $100M in subsequent years. The savings estimate is based on the $180 million identified in the federal audit report. It is expected that once these changes are implemented, cost avoidance savings will increase beyond these projections as pharmacy claims with improper DEA information continue to be rejected at the point-of-sale.

## Recommendation 4 – Publicize Drug Expiration Dates

***Enact legislation that requires the FDA to publish for public access the drug product expiration dates at the national drug code (NDC) level***

On November 1, 2010, the OIG released a report entitled *"Review of Terminated Drugs in the Medicare Part D Program."*[10] The report indicated that CMS accepted prescription drug event (PDE) data representing over $112 million in gross drug costs associated with 2,967 terminated drugs and recommended that "CMS issue regulations to prohibit Medicare Part D coverage of terminated drugs and, in the interim, publish a list of these drugs on its Web site." CMS rejected this recommendation, stating "[the] data source used in the report methodology is likely flawed..." and "...the only authoritative source of data on final product expiration dates at the national drug code (NDC) level is data officially submitted by manufacturers to the Food and Drug Administration (FDA)."

This White Paper recommends that legislation be enacted to require the FDA to publish drug product expiration dates at the NDC level. The result of this legislation would provide Medicare and Medicaid claims processors with the authoritative FDA data source that CMS recognizes. Claims processors would have the ability to establish a data edit that rejects prescription medication at the point of sale if the dispensing date exceeds the final product expiration date.

### Potential Savings

Recommendation 4 holds promise for generating up to $100M during initial implementation and up to $50M in subsequent years. The savings estimate is based on the $112 million that was identified in the OIG report. It is expected that once these changes are implemented, cost avoidance savings will increase beyond these projections as pharmacy claims for expired drugs continue to be rejected at the point-of-sale.

## Recommendation 5 – Match Vital Records to SSA and State MMIS

***Enact legislation that requires a nightly data feed from each state public health vital records office to the SSA Death Match File and the state MMIS***

On July 9, 2008, the Senate Subcommittee on Investigations released a report showing that between $60 million and $92 million was paid to Medicare recipients by deceased Medicare providers.[11] On September 30, 2009, the General Accounting Office (GAO) released a report showing that over $700,000 was paid for controlled substances on behalf of deceased Medicaid recipients or prescribed by deceased Medicaid providers.[12] Both reports reveal weaknesses in the system currently used to maintain provider and recipient date of death information.

Each state public health vital records office maintains death certificates that validate an individual's date of death. Providing a nightly data feed of accurate date of death information to the Social Security Administration (SSA) Death Match File and the state Medicaid Management Information System (MMIS) will significantly reduce the amount of payments made on behalf of deceased individuals. Accurate and up-to-date recipient and provider date of death data will allow Medicare and Medicaid claims to be rejected at point of submission rather than after the claim is paid (the standard "pay and chase" model).

### Potential Savings

Recommendation 5 holds promise for generating up to $100M during initial implementation and up to $50M in subsequent years. The savings estimate is based on the $60 - $92 million that was identified in the Senate Subcommittee on Investigations report. It is expected that once these changes are implemented, cost avoidance savings will increase beyond these projections as all claims that use the name of a deceased provider or recipient continue to be rejected at the point-of-sale.

## Recommendation 6 – Require Provider Re-enrollment

***Establish a mandatory re-enrollment program for all Medicaid providers***

Title 42 of the Code of Federal Regulations, Section 424.515 requires all providers and suppliers who currently bill the Medicare program to enter into a 5-year revalidation cycle once a completed enrollment application is submitted and validated. On March 25, 2011, CMS strengthened the provider enrollment process by expanding Sections 19 – 19.4, Chapter 15 of the *Medicare Program Integrity Manual*.[13] The *Medicare Program Integrity Manual* requires newly enrolled providers to be evaluated and then monitored based on one of the following three risk levels: limited, moderate, or high. This newly enacted requirement holds promise for minimizing potential abuse in the Medicare program.

The provider enrollment process can be strengthened further by enacting a mandatory provider re-enrollment program for all Medicaid providers. This White Paper recommends that the re-enrollment program be staggered over a multi-year period by provider type in order to reduce the administrative burden on individual states.

A few of the significant benefits that would be obtained from this continuous program include:

- Removal of non-existent, inactive, retired, or deceased providers from the Medicaid rolls
- Validation and update of professional licensure information for each active provider
- Validation and update of provider demographic information
- Validation and update of respective provider databases with current information

### Potential Savings

Recommendation 6 would bring about cost-avoidance savings resulting from the cleansing of Medicaid provider data through the re-enrollment process.

## Recommendation 7 – Publish National and State Healthcare Statistics

***Calculate and publish national and state-wide healthcare statistics***

The DOJ, FBI, and OIG are using advanced data analysis techniques to evaluate healthcare claims. These techniques include identifying high-billing levels in healthcare fraud "hot spots," so that analysts can target emerging fraud schemes. On February 28, a Texas physician and several accomplices were arrested in a nearly $375 million healthcare fraud scheme that was identified due to a fraud hot spot. The fraud analysts discovered that in 2010, while 99 percent of physicians who certified patients for home health signed off on 104 or fewer people, the indicted physician certified more than 5,000 individuals.[14]

This White Paper recommends that national and state-wide healthcare statistics—as well as the statistical norms used to identify provider hot spots—be published. Healthcare fraud data analysts could use this information to identify trends and aberrations that may uncover potential abuses. This White Paper further recommends that the following steps be taken to provide healthcare fraud data analysts with additional information to uncover emerging schemes.

- Establish baseline thresholds by provider type at the Medicare and Medicaid level
- Update threshold list at least quarterly
- Publish threshold list on the CMS website

### Potential Savings

Recommendation 7 holds promise for increasing critical resources essential to healthcare data analysis, identifying emerging healthcare schemes, and generating additional savings for the Medicare and Medicaid programs.

## Recommendation 8 – Establish Central Repository of Fraud and Abuse Cases

***Establish an electronic central repository that contains the results of all healthcare fraud and abuse cases***

Multiple reports and press releases are published each year that provide valuable information concerning successful healthcare fraud investigations. Examples include the OIG Semi-Annual Report to Congress; the Health Care Fraud and Abuse Control Report; Medicare Fraud Alerts; and OIG, DOJ, and FBI press releases. In addition, information regarding fraud investigation at the state level is often included in these organizations' respective annual reports. Typically, the reports include details about the fraud scheme, including the type of fraud and how it was perpetrated.

This White Paper recommends the creation of a central electronic repository of all federal and state healthcare fraud cases. The repository would provide an educational resource for healthcare fraud analysts as they seek to learn about cases that may emerge in their regional area. The repository will also expand the analysts' data mining capabilities through the inclusion of specific codes and patterns that were identified in the case.

This White Paper recommends that the following fields be included in the data to facilitate searches on topics relevant to the researcher:

- Type of fraud scheme (for example, claim, multi-party, kickback)
- Type of case (Medicare or Medicaid)
- State of occurrence
- Provider type
- Case date

### Potential Savings

The electronic repository will allow the healthcare fraud analyst to promote a prevention-first approach through the creation of new controls identified in the repository.

## III. Conclusion

Assistant Attorney General Tony West recently stated, "Ultimately, however, the role that science plays in forming our policies and practices—that will depend on each of you: your commitment; your vigilance; your dedication to ensuring that our work to create a criminal justice system that is more effective, more efficient, more just, will rest not merely on a foundation of hope, or goodwill, or good intentions, but on a bedrock of integrity born of science and research."

*Partnership*, in its most positive context, is a term that evokes promise, strength, and hope. Successful partnerships—collaborations of entities that share common goals—can generate a synergy that enables multiple and sometimes disparate communities to not only achieve a common good but elevate the good to a new plateau.

The science of healthcare fraud control is incumbent on individuals engaged in active and innovative partnerships and research. Healthcare fraud is not static. The criminal mind is constantly looking for new ways and methods to take advantage of the payer's system. This White Paper is based on continual research into healthcare fraud issues and efforts made to strengthen the existing Medicare and Medicaid system. Leveraging the knowledge and forward-thinking insights gained by federal, state, and contractual partners will advance the cause to improve program integrity efforts, strengthen payment reforms, and enhance fraud and abuse enforcement efforts.

▪▪

## About the Author

Dan Olson, CFE, has worked for over 15 years in healthcare fraud examination following five years in auditing and compliance. Mr. Olson is certified by the Association of Certified Fraud Examiners and a member of the National Healthcare Anti-fraud Association, Institute of Internal Auditors, Princeton Global Networks, and the Cambridge Who's Who.

Mr. Olson began his groundbreaking work in the program integrity field when he was tapped by the OIG of the Illinois Department of Healthcare and Family Services to be part of a charter four-member think tank called the Fraud Science Team. The goal of the team was to prevent fraud at the front end through identification techniques such as prospective editing, trending analysis, and pattern recognition. The team collaborated with Dr. Malcolm Sparrow, an international expert in the field of fraud and abuse to prevent healthcare fraud. While Mr. Olson was part of the team, CMS recognized Illinois as a best practice state, due in part to the creation of the Fraud Science Team.

In 2007, Mr. Olson accepted the position of Director of Fraud Prevention at Health Information Designs (HID). At HID, Mr. Olson continues his research in fraud prevention, and drew from his extensive program integrity background to design HID's Web-based comprehensive surveillance utilization review system (SURS), **SURVEIL**®. Built on proven concepts and best practices, **SURVEIL** is the first SURS solution that includes a fully-integrated case management system, allowing organizations to track potential fraud or abuse cases from the point of discovery through the disposition of the case. Mr. Olson leads HID's multi-disciplinary Fraud Informatics Technology (FIT) team in the analysis of data and the identification of potential fraud and abuse.

Mr. Olson is committed to researching trends and developments in the areas of healthcare fraud and abuse and educating other members of the program integrity community as well as external stakeholders. In April 2010, Mr. Olson authored "Using Data Analytics to Fight Fraud and Abuse: A Call to Action," a White Paper that offers best practices for addressing the aggressive and changing tactics of perpetrators. At the request of members of the Congressional Subcommittee on Health, Mr. Olson twice presented "Spotlight on State Healthcare Fraud and Abuse" in 2011. In the months following these presentations, legislative staff members have sought Mr. Olson's professional opinion on healthcare fraud and abuse issues.

Mr. Olson writes a national monthly healthcare fraud newsletter for program integrity professionals, ***SURVEIL** Now*. Mr. Olson has been a featured speaker at the Eastern Medicaid Pharmacy Administrators Association (EMPAA) and American Drug Utilization Review Society (ADURS) conferences, presenting "The Science of Fraud Control and the Art of Discovery."

Mr. Olson also shapes the direction of fraud prevention initiatives by serving as a charter member on the Advisory Council for the Association for Certified Fraud Examiners and on the Advisory Council for Harvard Business Review.

Mr. Olson welcomes comments and the opportunity for further discussion. He can be reached at 601-420-4613 or dan.olson@hidinc.com.

# About Health Information Designs

As a leader in healthcare data analysis, Health Information Designs, LLC (HID) understands the challenges faced by Medicaid agencies and healthcare programs. For over 30 years, HID has provided drug utilization review, prior authorization, prescription drug monitoring, clinical support services, and technology solutions for clients in more than 29 states.

HID's Surveillance Utilization Review System (SURS), **SUR**VEIL, provides the solution to unravel complex and sophisticated fraud and abuse strategies in the healthcare system. **SUR**VEIL is a comprehensive exception processing system designed to identify patterns and trends that may lead to potential fraud and abuse. Conceived by a team of business and technical experts, including a nationally-recognized fraud and abuse expert, **SUR**VEIL optimizes the identification of potential fraud and abuse through the prospective identification of emerging fraudulent patterns and retrospective evaluation of paid and rejected claims data.

# Offices

## Corporate Office

391 Industry Drive
Auburn, AL 36832
Phone: 334.502.3262
Fax: 334.466.6947

## Maryland Office

213 West Main Street, Suite 204
Salisbury, Maryland 21801-4871

# Corporate Web Site

www.hidinc.com

***Do you need more information about fraud control?***

*HID's Fraud Informatics Technology team, led by Dan Olson, CFE, produces a monthly* ***SUR****VEIL newsletter. If you would like to receive this newsletter, please contact Mr. Olson directly at 601-420-4613 or dan.olson@hidinc.com.*

# End Notes

1. http://www.justice.gov/iso/opa/ag/speeches/2012/ag-speech-120214.html
2. https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/FraudAbuseforProfs/Downloads/fy09spiaexecsum.pdf
3. http://www.fbi.gov/seattle/press-releases/2012/south-sound-doctor-sentenced-to-more-than-12-years-in-prison-for-health-care-fraud-tax-crimes-and-drug-distribution
4. http://www.fbi.gov/news/pressrel/press-releases/medicare-fraud-strike-force-charges-91-individuals-for-approximately-295-million-in-false-billing?utm_campaign=email-Immediate&utm_medium=email&utm_source=national-press-releases&utm_content=30298
5. http://www.hhs.gov/news/press/2011pres/02/20110217a.html
6. http://www.justice.gov/opa/pr/2012/February/12-crm-260.html
7. http://www.fbi.gov/news/news_blog/strike-force-takedown-050212
8. http://www.gao.gov/new.items/d11822t.pdf
9. http://www.whitehouse.gov/the-press-office/presidential-memorandum-enhancing-payment-accuracy-through-a-do-not-pay-list
10. http://oig.hhs.gov/oas/reports/region7/70903130.pdf
11. http://www.hsgac.senate.gov/search/?q=deceased+doctors&search-button=Search&access=p&as_dt=i&as_epq=&as_eq=&as_lq=&as_occt=any&as_oq=&as_q=&as_sitesearch=&client=hsgac&sntsp=0&filter=0&getfields=&lr=&num=15&numgm=3&oe=UTF8&output=xml_no_dtd&partialfields=&proxycustom=&proxyreload=0&proxystylesheet=default_frontend&requiredfields=&sitesearch=&sort=date%3AD%3AS%3Ad1&start=0&ud=1
12. http://www.gao.gov/new.items/d091004t.pdf
13. https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNMattersArticles/downloads/MM7350.pdf
14. http://www.hhs.gov/news/press/2012pres/02/20120228d.html

# Using Data Analytics to Fight Fraud and Abuse: *A Call to Action*

**Dan Olson**
with Connie Lewis, MBA

April 2010

HEALTH INFORMATION DESIGNS

## Contents

***Recent federal directives have turned a national spotlight on the issue of fraud and abuse in the health care system. In this paper, the author—a distinguished member of the Program Integrity community—explains that the only recourse for fraud control professionals is to continually alter their methods and tactics to stay one step ahead of perpetrators. Advancements in information technology, coupled with expert logic, provide improved methods for targeting and identifying fraud, and recouping damages. Using these methods, fraud control professionals should move beyond the status quo and stay poised to fight fraud not only as it exists but as it emerges.***

# I. Background

The year 2009 will be remembered for the historic strides that took place in the examination of the health care industry. The debate on health care reform permeated the news media on a routine basis as congressional leaders researched, debated, and worked to craft a federal plan that would serve the neediest constituencies.

The debate appropriately cast a spotlight on health care fraud and abuse, bringing the issue to national attention. On January 28, 2010, the first National Summit on Health Care Fraud was held in Bethesda, Maryland. At the summit, Acting Deputy Attorney General Gary Grindler provided this telling statement during his opening remarks:

> *It is not enough just to prosecute and punish health care fraud after it occurs. We must target it before it happens through aggressive pre-screening, auditing, and prevention techniques. We need to use the most effective technologies available to provide real-time access to claims data and to conduct effective data analysis so that we can detect new fraud schemes as they emerge. And we need to leverage our civil, criminal and administrative enforcement authorities along with building effective public-private partnerships.*[1]

Less than two months later, President Barack Obama issued a memorandum to increase the collection of improper health care payments through "Payment Recapture Audits," described as audits conducted using state-of-the-art technology and expert professionals to ferret out fraud and abuse.[2] The potential recovery from this effort is anticipated to be at least $2 billion over the next three years.

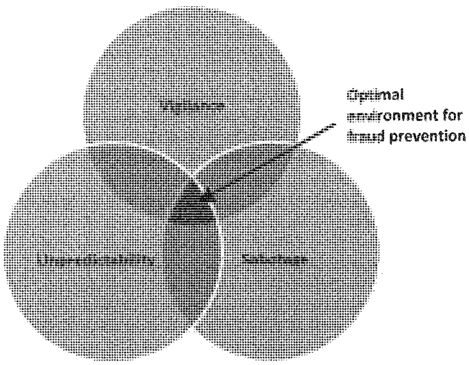
The recent directives regarding health care fraud and abuse represent a direct **call to action**. While fraud control professionals should continue their standard operating procedures, they must not be complacent with maintaining the status quo. Instead, program integrity departments must strengthen their efforts by finding new approaches and angles to identify and prosecute fraud and abuse cases, and proactively prevent future cases. The remainder of the paper is dedicated to explaining the optimal approach to fighting fraud using **data analytics**, which integrates advanced database technology with expert, industry-based logic.

## II. Vigilance, Unpredictability, and Sabotage

Health care *fraud* amounts to the intentional misrepresentation of a material fact on a health care claim in order to persuade the payer to process and pay a false claim. Health care *abuse* is a disregard for accepted business or medical practices in order to obtain a greater claim reimbursement.

Traditionally, both fraud and abuse were identified through analysis of paid claims data. This approach is not enough. Today's fraud control professionals cannot simply perform static, post-payment reviews. A contemporary and comprehensive approach must utilize multiple approaches to address emerging issues of fraud and abuse to thwart would-be perpetrators from siphoning Medicare and Medicaid dollars from needy citizens. As fraud expert Dr. Malcolm Sparrow points out, the compelling nature of fraud control demands vigilance, unpredictability, and sabotage in responding to emerging patterns of fraud.[3]

- **Vigilance** – The fraud control professional must be vigilant—ever-seeking new possibilities or angles that allow fraud and abuse to be identified as it is occurring and before the claim is paid. Without vigilance, the fraud control professional becomes complacent in relying on methods of fraud control that worked in the past, without modifying or supplementing these to address new methods used by fraud perpetrators.
- **Unpredictability** – Predictable—or static—patterns of behavior on the part of the fraud control professional provide an opportunity for innovative fraud perpetrators to develop schemes that will leech untold dollars from payers. Conversely, unpredictable or creative patterns of behavior create an imbalance for fraud perpetrators that will confuse and possibly defuse their planned fraudulent activities. Fraud and abuse control professionals must alter and vary their behavior to keep their detection methods unpredictable.



- **Sabotage** – The fraud control professional must be nimble, in order to counteract emerging fraud and abuse schemes by sabotaging them early in their development. Various forms of sabotage are effective in subverting the activity of a perpetrator. For example, one method (that will quickly elicit a response from the perpetrator) is to suspend payments pending a review of claims. The fraud control professional can also work with law enforcement officials to coordinate undercover work to build a case against the perpetrator.

While each of these factors is significant individually, the combination of the three produces the best possible climate for identifying cases of fraud and abuse and potential acts of fraud and abuse. Fraud control professionals should work diligently to achieve this optimal environment. The absence of these factors will provide a greater opportunity for a fraud perpetrator to exploit the weaknesses of health care payment systems.

# III. Using Data Analytics to Detect and Prevent Fraud

Fraud control in the health care system involves the objective, careful, and systematic study of health care data. By running large amounts of data against algorithms carefully crafted to uncover unscrupulous acts, analysts can pinpoint cases of potential fraud or abuse for follow up and further investigation.

*The answers are in the data.*

It has been aptly said that the "answers are in the data." While simply put, this is a profound truth. However, data will reveal the correct answers only when the correct questions are asked and the results are properly evaluated. The following points should guide the work of data analysis:

- What are the key questions that need to be asked?
- How should the data be evaluated?
- How much effort should we expend to find answers?

## Asking the Right Questions

For each submitted claim, the fraud control professional must ask several key questions to begin the evaluation process.

***Is this a valid claim?*** In the most elementary sense, a valid claim is one that passes successfully through claims processing front-end edits. However, to determine real validity, the fraud control professional must continue questioning.

***Is the claim legitimate? In other words, was it properly submitted for medically-necessary services rendered on behalf of a beneficiary?*** To determine the validity of a submitted claim, the claim must be evaluated within its context, which encompasses the services surrounding the claim submittal and the claim demographic. If the surrounding services are consistent with the claim in question and comply with medical standards, then the claim's validity is increased. However, if there are inconsistencies in the surrounding services, then the fraud control professional should question the claim's validity. The claim demographic can take on many layers, such as transaction type (e.g., professional, institutional, pharmaceutical); provider type (e.g., pharmacy, laboratory); or beneficiary category of eligibility (e.g., illegal alien, working disabled). Inconsistencies in the claim demographic, when taken in context with the surrounding services, should cause the fraud control professional to question the claim's validity. The context of the claim is critical in determining the validity of the claim submittal.

***Is the claim a legitimate claim in relation to the payer's payment policy?*** Policy manuals, provider handbooks, state and federal regulations, etc. dictate the proper method of payment for a claim. Embedded within the payment policy are business rules that define procedures, thresholds and limits for the payment of the claim. The payment policy is the linchpin that defines the proper payment edit structure. Consistency between the payment policy and the payment edit structure is monumental when validating a claim. When consistency breaks down, loopholes are created and the payer's system becomes vulnerable for potential fraud and abuse.

## Using the Right Methods

It is important to remember that each claim is unique. However, beyond this uniqueness, a body of claims will exhibit characteristics that allow the fraud control professional to explore the data and look for revealing trends and patterns of behavior. These trends and patterns become the basis for discovering predictive behavior that will lead to unraveling an emerging fraud or abuse scheme before it occurs.

Trends and patterns on their own do not necessarily indicate bad or flawed behavior. For instance, one might find that a provider's or clinic's billing practice will only submit claims for payment at the end of each month. On its own, this may not reveal a questionable practice, especially if the dates of service for these claims occurred in the previous 30 – 60 days. However, the results of the analysis would change if the dates of service were consistently for claims eight to twelve months old, or perhaps for claims that had been previously rejected multiple times.

Traditional surveillance utilization review systems' (SURS) exception processing will allow the fraud control professional to identify statistical outliers based on standard deviations. A statistical outlier in its purest form is data (or claims) that have separated themselves from the normal distribution of the data. The separation of data could occur at the upper- or lower-bound of the data spectrum. For example, an exception process might identify family practitioners who exceed the standard deviation and consistently submit claims for the most expensive established office visit procedure code, i.e., 99215.

Recently, the Medicare Fraud Strike Force used this process to identify statistical outliers that exceeded the national averages for specific claims. The Medicare Fraud Strike Force called these aberrations "fraud hot spots." For example, when the Strike Force calculated the amount paid per beneficiary for inhalation drugs in Miami and compared it to the national average, they discovered that Miami exceeded the national average by 3,000%. The Strike Force also calculated the number of eye tests performed in Houston and compared it to the national average for eye tests performed, finding that the number of eye tests performed in Houston exceeded the national average by 2000%.[4] The criminal mind is constantly looking for new ways and methods to take advantage of the payer's system. It is incumbent on the fraud control professional to expand beyond statistical outliers to address other potentially abusive areas.

> *The criminal mind is constantly looking for new ways and methods to take advantage of the payer's system.*

**The vigilant fraud control professional must implement a multi-faceted approach to evaluate the data.** The following are examples of areas in which research should be expanded:

- **Inter-relationships** – This area involves evaluating a beneficiary's relationship with multiple providers to identify a potential kickback scheme or duplicate billings. The kickback scheme may be identified through examination of the provider-beneficiary relationship. For example, analysis of a nursing home may result in a discovery that all beneficiaries are treated by the same physician clinic, serviced by the same transportation company, and receive medications from the same pharmacy. Further review may determine that ownership interests are intertwined between all providers involved or that kickbacks are being given to secure a provider's business.

  A duplicate billing scheme can also be identified through examination of the provider-beneficiary relationship. A cluster of beneficiary claims for the same service may be submitted by several providers on the same date of service. The perpetrator may try to disguise the duplicate billings by submitting claims for payment at different times, e.g., different months. A second example may be identified when a beneficiary list is passed around a clinic or group practice, and claims are submitted by multiple providers for the beneficiaries with the same procedure code on the same date of service.

- **Newly Enrolled Provider Monitoring** – This area involves evaluating newly-enrolled providers within the bounds of their provider type. Knowledge of the data is essential in order to understand the typical growth pattern that a newly-enrolled provider may exhibit within their provider type. The analysis would begin once the newly-enrolled provider begins to submit claims. Providers would be flagged for review at any point they exceeded the growth pattern during the evaluation period.

- **Quality of Care** – This area involves examining beneficiary claims to determine if the beneficiary received an established standard of care for their medical condition. For example, an expectant mother should receive a minimum number of office visits, sonograms, and lab tests during the course of her pregnancy. If these standards are not met, then a quality of care issue could be raised. Quality of care can also be reviewed in a managed care environment to determine if an underutilization of services occurred.

> *Continual vigilance ... will counteract the criminal mindset.*

Would-be perpetrators will initially be caught off-guard by these approaches, but they will quickly adapt and redirect their criminal activity to new areas of exploitation. It is important to note that a multi-tier analytical approach must be ongoing. Continual vigilance, unpredictability, and sabotage at multiple data levels—transaction, group and multi-party—will counteract the criminal mindset.

## Expending the Right Efforts

Achieving success in the identification of health care fraud and abuse is dependent upon the level of effort and resources that are allocated. A commitment to the acquisition of proper technologies, the proper staffing, and a far-reaching think-tank approach will garner success in derailing fraudulent and abusive activity.

- **Proper Technologies** – The acquisition of effective technologies that provide real-time access to data and conduct effective data analysis is an essential step in subverting health care fraud and abuse. These tools must have the ability to use data analytics to perform statistical analysis at multiple levels to reveal aberrant behavior and facilitate predictive modeling. The ability to drill down to the claim line detail to identify the claim demographic is inherent in this process. The technology must also have the ability to efficiently track all segments of activity on each case from inception through disposition.

- **Proper Staffing** – The establishment of multiple partnerships among government, law enforcement, and fraud control professionals creates a synergy that will lead to increased integrity efforts and advance the overall cause of fraud prevention. Development of a prevention-first mindset will lead to an efficient and effective avenue to identify fraud and abuse schemes as they emerge.

Initial success in closing loopholes in the payment system, sabotaging emerging fraudulent or abusive schemes, or terminating providers will validate the work that has been accomplished. Caution must be taken to avoid complacency in the continual pursuit of emerging fraudulent and abusive practices. True success will occur when the level of effort is sustained and health care fraud and abuse is reduced.

## IV. Conclusion

Agencies are under great pressure to reduce health care costs by not only recovering improper payments, but by stopping fraud and abuse before it occurs. This cannot be done without investing in the best technological tools available and employing expert fraud control professionals to harness them. A contemporary and comprehensive approach to fraud control incorporates data analytics to discover issues as they emerge, track perpetrators, and ultimately recover overpayments.

*Fraud control professionals must leverage the power of data analytics and statistical profiling ...to combat and disrupt emerging issues in health care fraud and abuse.*

Returning to Acting Deputy Attorney General Grindler's statement:

> *It is not enough just to prosecute and punish health care fraud after it occurs. We must target it before it happens through aggressive pre-screening, auditing, and prevention techniques. We need to use the most effective technologies available to provide real-time access to claims data and to conduct effective data analysis so that we can detect new fraud schemes as they emerge. And we need to leverage our civil, criminal and administrative enforcement authorities along with building effective public-private partnerships.*

The significance of this statement strikes at the core of our responsibility as program integrity professionals. We must leverage the power of data analytics and statistical profiling, and collaborate with stakeholders and law enforcement, to provide an intentional vigilance in our mission to combat and disrupt emerging issues in health care fraud and abuse.

## About the Author

Dan Olson has worked for over a decade in fraud examination following five years in auditing and compliance. Mr. Olson began his groundbreaking work in the program integrity field when he was tapped by the Office of Inspector General (OIG) of the Illinois Department of Healthcare and Family Services to be part of a charter four-member think tank called the Fraud Science Team. The goal was to prevent fraud at the front end through identification techniques such as prospective editing, trending analysis, and pattern recognition. While Mr. Olson was part of the team, the Centers for Medicare & Medicaid Services (CMS) recognized Illinois as a best practice state due in part to the creation of the Fraud Science Team.

Mr. Olson is known in the national program integrity arena for authoring a White Paper in 2005 that provided recommendations to improve the integrity of the National Provider ID. While in Illinois, he also served as a charter member of the Medicaid Fraud Prevention Executive Workgroup, performing pharmaceutical research and developing several prospective edits that saved the State of Illinois millions of dollars.

Currently the Director of Fraud Prevention at Health Information Designs, Inc. (HID), Mr. Olson is a member of the Association of Certified Fraud Examiners, the Institute of Internal Auditors and the Princeton Global Networks. Within the past year, Mr. Olson was a featured speaker at the National Association for Medicaid Program Integrity (NAMPI) annual conference and presented "The Science of Fraud Control and the Art of Discovery" at the Eastern Medicaid Pharmacy Administrators Association (EMPAA) and American Drug Utilization Review Society (ADURS) annual conferences.

Dan Olson's work with fraud prevention logic provides the ideal background for designing technology to detect, address, and prevent fraud. Since moving to HID in 2007, Mr. Olson has employed his impressive background in program integrity to design HID's comprehensive Web-based SURS and Case Management solution, **SUR**VEIL™. Built on proven concepts and best practices, **SUR**VEIL is the first solution to integrate a full case management system within a surveillance utilization review system, allowing organizations to track potential fraud or abuse cases from the point of discovery through the disposition of the case.

Mr. Olson welcomes comments and the opportunity for further discussion. He can be reached at 601-420-4613 or dan.olson@hidinc.com.

## About Health Information Designs

As a leader in healthcare data analysis, Health Information Designs, Inc. (HID) understands the challenges faced by Medicaid agencies and healthcare programs. For over 30 years, HID has provided drug utilization review, prior authorization, prescription drug monitoring, clinical support services, and technology solutions for clients in more than 20 states.

HID's **SURVEIL**™ Surveillance Utilization Review System (SURS) provides the solution to unravel complex and sophisticated fraud and abuse strategies in the healthcare system. **SURVEIL** is a comprehensive exception processing system designed to identify patterns and trends that may lead to potential fraud and abuse. Conceived by a team of business and technical experts, including a nationally-recognized fraud and abuse expert, **SURVEIL** optimizes the identification of potential fraud and abuse through the prospective identification of emerging fraudulent patterns and retrospective evaluation of paid and rejected claims data.

## Offices

### Corporate Office

391 Industry Drive
Auburn, AL 36832
Phone: 334.502.3262
Fax: 334.466.6947

### Mississippi Office

513 Liberty Road, Suite 2A
Flowood, Mississippi 39232

### Maryland Office

213 West Main Street, Suite 204
Salisbury, Maryland 21801-4871

## Corporate Web Site

www.hidinc.com

***Do you need more information about fraud control?***

*HID's Fraud Informatics Team, led by Dan Olson, produces a monthly **SURVEIL** newsletter. If you would like to receive this newsletter, please contact Mr. Olson directly at 601-420-4613 or dan.olson@hidinc.com.*

# End Notes

1. U.S. Department of Health and Human Services and U.S. Department of Justice, "Stop Medicare Fraud," (http://www.stopmedicarefraud.gov/healthcarefraud.html)

2. Presidential Memorandum Regarding Finding and Recapturing Improper Payments, March 10, 2010. (http://www.whitehouse.gov/the-press-office/presidential-memorandum-regarding-finding-and-recapturing-improper-payments)

3. Sparrow, Malcolm K. *The Character of Harms: Operational Challenges in Control.* Cambridge University Press, 2008

4. Prepared comments by Assistant Attorney General Lanny Breuer at the 2009 National Health Care Anti-Fraud Association Conference on November 18, 2009.

Mr. PITTS. Ms. Lavelle, you are recognized for 5 minutes for an opening statement.

## STATEMENT OF ALANNA M. LAVELLE

Ms. LAVELLE. Thank you.

Chairman Pitts, Ranking Member Pallone, and members of the subcommittee, I am Alanna Lavelle, director of special investigations for WellPoint. Thank you for the opportunity to provide our input and recommendations on detecting and deterring fraud and abuse in the healthcare system.

Healthcare fraud is not a victimless crime. We all pay, and we pay dearly. Costs extend beyond financial loss. People are harmed by wasteful, inappropriate testing and treatment.

One of the significant strengths that we and other health plans provide is the data available from our integrated healthcare benefits. This allows us the ability to see the entire healthcare spectrum and to spot trends and outliers.

We also have a dedicated fraud and abuse prevention team, known as the Special Investigations Unit, SIU. I am one of the lead investigators, and we are staffed by former Federal and State law enforcement agents and medical professionals. We also have a data analysis team.

Our goal at WellPoint is to prevent healthcare fraud and abuse for the benefit of our members' health. And in order to meet this goal, we have developed a number of different types of programs to identify and prevent healthcare fraud and abuse, three of which I will briefly describe.

First, we have our Controlled Substance Utilization Monitoring Program and our Medicaid Restricted Recipient Program. Prescription narcotic drug abuse is a national epidemic today. Through these programs, we are helping identify those who are engaged in or contributing to prescription drug abuse and/or drug diversion.

For example, for our Medicaid plans, we have implemented a restricted recipient program in which a member who within a 3-month period visits 3 or more prescribers, 3 or more pharmacies, and fills 10 or more controlled substance prescriptions without a confirmed underlying medically necessary condition, and we lock them into using only 1 primary care physician as prescriber, 1 retail pharmacy of their choice, and 1 hospital. Our case managers work directly with providers and members. And to date, the program has saved lives and many millions of dollars in emergency department visits alone for drug-seeking behavior.

Second, we have recently contracted with a vendor to do predictive modeling at WellPoint. The program uses advanced neural network technology from FICO to identify previously unknown and emerging fraud and abuse provider and member schemes. Suspect providers and claims are reviewed to identify potential fraud, waste, or abuse and investigated thoroughly. Since we began using this tool just 6 months ago, we have opened 90 investigations and have achieved $27 million in projected savings. The return on the investment at this time is well over 15 to 1.

And, finally, we take a multifaceted approach to identify bogus providers who do not actually perform services for real patients. Our provider database team alerts our investigators as to the presence of new claims coming in for new labs, new pharmacies, and new durable medical equipment suppliers, or DMEs. And we provide a full background check as well as a drive-by of the provider's purported office space. To date, in the State of California alone, we at WellPoint have stopped over 239 bogus DME providers before they were able to defraud us.

So based on our experience in combating healthcare fraud and abuse, we offer the following recommendations to enhance future efforts throughout all sectors of health care.

First, we are supportive of giving CMS the authority to establish a restricted recipient program in Medicare Part D for those beneficiaries displaying a pattern of misutilization.

Second, we recommend that dually eligible beneficiaries with evidence of drug-seeking behavior should be locked into one managed care plan, rather than continue to be allowed to switch plans on a monthly basis to evade detection.

Third, we support better coordination and cooperation among CMS, DOJ, and all stakeholders.

And, finally, all expenses for health insurers' antifraud and -abuse programs should be included as activities that improve healthcare quality in the medical loss ratio calculation since they reduce waste, which reduces the cost of health care, and enhance patient safety by helping identify and remove providers engaging in unsafe and fraudulent practices from the healthcare system.

In conclusion, I would like to thank the committee for the opportunity to testify today on behalf of WellPoint on this critical issue and pledge our support in any efforts to make the healthcare system financially viable and safe for our members.

[The prepared statement of Ms. Lavelle follows:]

TESTIMONY

# Examining Options to Combat Health Care Waste, Fraud and Abuse

**Ms. Alanna M. Lavelle**
**Director, Special Investigations**
**WellPoint, Inc.**
**3350 Peachtree Road, Atlanta, GA 30326**

**Subcommittee on Health**
**Energy & Commerce Committee**
**U.S. House of Representatives**

**Wednesday, November 28, 2012**

Chairman Pitts, Ranking Member Pallone, and Members of the House Energy and Commerce Subcommittee on Health, I am Alanna Lavelle, Director of Special Investigations for WellPoint, Inc. WellPoint is one of the nation's largest health benefits companies with more than 33 million people in our affiliated health plans, and approximately 64 million people served through our subsidiaries. I joined WellPoint in 2004 after serving 25 years with the FBI. My experience in the FBI included managing a national health care fraud case during the critical Columbia/HCA investigation, and I initiated the first Health Care Fraud Task Force in Texas. I also served as the Supervisory Special Agent FBI liaison for the Centers for Disease Control (CDC), working closely with the CDC on Bioterrorism matters in the post 9/11 era. I am a registered mediator and a Certified Professional Coder. I hold a M.S. in Conflict Management and a B.A. in International Relations. I also serve on the Data Analysis and Review Committee of the Healthcare Fraud Prevention Partnership, a voluntary public-private partnership recently organized for the purposes of reducing the prevalence of health care fraud. Recently I was named Chair of the National Health Care Anti-Fraud Association, the leading national association composed of both private and public sectors focused exclusively on fighting health care fraud and abuse.

Thank you for the opportunity to provide our input and recommendations on detecting and deterring fraud and abuse in the health care system. We appreciate your leadership on addressing what we believe to be a critically important issue: protecting patient safety and the financial viability of our health care system through detecting and deterring health care fraud and abuse. At a time of rising health care costs, it is essential not only to stop the costly drain on the U.S. health care system, but also to protect consumers' health and safety.

## General Principles

In order to truly make inroads into the problems associated with health care fraud and abuse, WellPoint believes that a holistic view needs to be adopted, since the enormous costs of health care fraud and abuse are borne by all Americans whether they have private health insurance coverage or government-provided health care. Health care fraud and abuse is not just a Medicare or Medicaid problem – it is a health care system problem and it is the American taxpayer who is paying for it. Moreover, it is clear that many of the same individuals and entities that perpetrate fraud against government health care programs also engage in fraudulent activity in the private health insurance industry. Thus, the most effective way to address health care fraud and abuse is to forge a close and active partnership between private health plans, government agencies, and the provider community. It is only through cooperation and collaboration between the public and private sectors that health care fraud and abuse can be meaningfully addressed.

In addition, it is important to understand that stopping health care fraud and abuse means that multi-faceted approaches need to be used, as there is more than one problem and more than one source. For example, drug fraud or abuse can be caused by overutilization (drug abuse) or fraudulent prescribing (for financial gain), and can be driven not only by the recipients of the drugs but also by prescribing providers. For this reason, it is important to recognize that a one-size fits all solution does not exist. Congress, the Administration, and the agencies of jurisdiction need to increase their collaboration with each other and with the private sector in order to combat fraud and abuse throughout the health care system.

**WellPoint's Experience**

One of the significant strengths that WellPoint and other health plans provide is the data available from our integrated health care benefits. This allows us the ability to see the entire health care spectrum and to spot trends and outliers – such as the overprescribing physician or the patient receiving multiple prescriptions from multiple providers or pharmacies. For WellPoint's members that have both pharmacy and medical coverage under WellPoint, we have been able to identify:

- Provider practice patterns regarding the overprescribing of medications or performing unnecessary surgeries or procedures;
- Inappropriate coding by providers to receive greater reimbursement or reimbursement for services not rendered;
- Members in crisis or at risk of harmful prescription drug use, including abusive or potentially addictive usage patterns;
- Members who may benefit from chemical dependency and/or pain management intervention to improve quality of life; and
- Criminal enterprise and/or individuals defrauding the health care system, through the work of our fraud and abuse Special Investigations Unit (SIU).

**WellPoint's Special Investigations Unit**

To enhance our efforts to combat fraud and abuse, WellPoint has a dedicated fraud and abuse prevention team known as the Special Investigations Unit (SIU). I am one of the lead investigators, overseeing a team in the Southeast region. The SIU, led by a former Los Angeles Assistant United States Attorney, is staffed with employees having prior experience in the FBI, state law enforcement, and state insurance department fraud units. Medical professionals, including doctors and nurses who have clinical and coding expertise, also work within the SIU. Finally, the data analysis team is comprised of individuals with IT or other computer-related backgrounds. The investigators are responsible for investigating assigned cases in order to detect fraudulent, abusive or wasteful activities/practices and recover funds paid on such claims. Our programs at WellPoint also include collaborative efforts between our SIU and our contracted pharmacy benefit manager, Express Scripts, to identify retail pharmacies cooperating with over-prescribing or inappropriate prescription patterns and to exclude such pharmacies from our provider networks.

## WellPoint's Successful Fraud Prevention Programs

Our goal at WellPoint is to prevent health care fraud and abuse for the benefit of our members' health, as well as for the health care system as a whole. In order to meet this goal, WellPoint has developed a number of different types of programs to identify and prevent health care fraud and abuse, a few of which are discussed below.

### 1. Controlled Substance Utilization Monitoring (CSUM) Program

Our nation has a significant problem with prescription narcotic drug abuse and patients have at times gamed the system by doctor shopping, making multiple emergency room visits, and obtaining multiple prescriptions for narcotic drugs. Through a Controlled Substance Utilization Monitoring Program, (CSUM), health insurers can aid in patient safety and identify those who are engaged in or contributing to prescription drug abuse.

Our CSUM program in our commercial and Medicare business identifies members who, within a three month period, visit three or more prescribing providers, visit three or more pharmacies, and have filled ten or more controlled substance prescriptions (narcotics, benzodiazepines and hypnotics) without a confirmed underlying medically necessary condition (such as cancer or multiple sclerosis) to justify numerous controlled substances. The goal is to prevent members who have exhibited a pattern of obtaining multiple prescriptions for controlled substances from different providers and multiple dispensations of these medications from continuing to obtain inappropriate amounts and dosages of drugs through their health care coverage. Members who are identified through this program are alerted to oversight of their Schedule II prescription drug activity and case managed. To date, the program has been very successful; for example it has helped saved millions of dollars in emergency department visits for drug-seeking behavior. There has not been significant abrasion, and in fact some members have found the program helpful in managing their treatment.

2. Medicaid Restricted Recipient Program

WellPoint has also implemented a restricted recipient program for our Medicaid plans in Indiana called The Right Choices Program," and in Virginia called "RX Safe Choice," in which a member who has been identified as an abuser or at risk for abuse of controlled substances can be restricted to the use of only one primary care physician, one retail pharmacy, and one hospital for any non-emergency care. Our case managers, who work specifically with both the Indiana and Virginia membership, work directly with providers and members regarding excessive controlled substance use. Once a member is placed in the program, the primary medical provider must approve all referral providers for the member. Efforts are made to connect members with behavioral health providers, case managers and community resources related to abuse and addictions.

3. Provider Engagement in the Prescription Drug Trade

Provider involvement in the prescription drug trade of narcotics and other expensive drugs is a serious problem in our country, in particular in the state of California. As noted in last week's November 11, 2012 Los Angeles Times article, "federal researchers reported that emergency room visits resulting from the non-medical use of opiod prescription drugs - often used in pain relief - more than doubled from 2004 through 2008. There were as many visits for those prescription medications as for illegal drugs.[1]" Times reporters analyzed 3,733 prescription drug-related deaths in four Southern California counties, revealing that just 71 doctors - one-tenth of one percent in those counties- had written prescriptions in 17 percent of such fatalities over six years. WellPoint SIU plays an instrumental part in identifying to California law enforcement agencies those prescribers of narcotics to individuals with no underlying medical conditions, because we have access not only to the pharmacy information, but also the medical records of the recipients of the narcotics and are able to see trends and outliers. We provide quarterly reports identifying the top prescribers in each California county, and prepare individual reports where the recipients of the narcotics do not have underlying medical conditions.

4. Pre-pay provider review program

Part of WellPoint's antifraud program activities includes examining physician practice patterns, to determine whether outlier physicians whose practices are different from the norm are engaging in questionable behavior that not only are driving up costs, but also are impacting patient safety. WellPoint investigators are able to identify aberrant provider practice patterns through data mining and analytics in which they look for outlier activities such as significant dollar spikes in payments or cumulative dollar spikes in certain counties. WellPoint has

[1] Los Angeles Times, November 11, 2012; "Legal Drugs, Legal Outcomes," by Scott Glover and Lisa Girion

implemented two such pre-pay provider review programs in which the most egregious billers who, after being educated and refusing to modify their billing behavior, are placed on "Flagged Pre-Payment Review." For example, providers are identified as outliers if they show patterns of engaging in billing practices that are extremely aberrant compared to their specialty peers. "Upcoding" (coding a less intensive service as a more intensive procedure), billing an incorrect code to obtain coverage for a noncovered service, or billing at a particular facility to obtain extra reimbursement (e.g., billing a simple toenail clipping performed in an outpatient facility as debridement performed at an ambulatory surgery center) are examples of such outliers.

If a provider shows a pattern of engaging in such outlier behavior, WellPoint investigators and Medical Directors intervene to communicate with the provider to educate and attempt to correct his or her behavior if appropriate. About 60 percent of providers change their practices within 90 days after receiving such communications. However, the 40 percent of providers that continue to engage in incorrect coding may be placed on pre-pay review. In that case, providers must bill with paper claims accompanied by medical records so that we can determine whether the procedures billed for are reflected in the records.

5. Predictive modeling program

WellPoint has recently contracted with a vendor to provide an automated solution to enable WellPoint to continuously monitor medical (professional claims on CMS 1500s) claims across the company in a post-payment or future pre-payment environment. The initial rollout focuses on deploying the solution in the post-payment environment. WellPoint initially rolled out the program in Georgia, with the intent to implement it enterprise-wide in 2013.

The program uses advanced neural network technology from FICO[2] to identify previously unknown and emerging fraud and abuse provider/member schemes. FICO-based analytics score suspect claims on a scale of 1-1000 and identify aberrant provider/member behaviors. Suspect providers and claims are reviewed by a triage unit and the SIU to identify potential fraud, waste or abuse, and depending on the type of findings are then assigned to the investigative unit to investigate, prevent and stop ongoing fraud and abuse.

Since we began using this tool six months ago, WellPoint's SIU has opened 90 investigations and has achieved $27 million in projected savings. For example, the program has revealed patients with consecutive days of anesthesia, which is not medically likely, as well as lab testing for cardiac risk or food sensitivities where labs were billing for hundreds of units of antigens. The program has also identified certain weaknesses in our systems and procedures, which we then work quickly to strengthen.

6. Bogus providers

Bogus providers are those providers that, although they may have National Provider Identifier numbers (which are usually stolen or purchased), do not actually perform services for real patients. Instead, bogus providers steal or purchase patient identification numbers, establish a fake storefront office furnished with limited inventory, obtain a post office box, and proceed to bill insurers for fraudulent services and devices. Bogus providers are a significant problem in both commercial health insurance as well as in the Medicare Advantage program.[3]

[2] FICO is the acronym for Fair Isaac Corporation, which provides analytics and decision making services to assist financial services organizations in making complex, high volume decisions.

[3] Of note is that Section 6401 of the Affordable Care Act provides for a ninety-day period of enhanced oversight for the initial claims of DME suppliers where HHS suspects there may be a high risk of fraudulent practices.

WellPoint takes a multifaceted approach to identifying bogus providers and preventing their fraudulent billing. SIU's Provider Database team alerts investigators to the presence of new labs, pharmacies and durable medical equipment (DME) clinics, and performs a full background check as well as a drive-by of the provider's purported office space. WellPoint also matches U.S. Post Office box numbers against our current claims to determine whether multiple bogus providers are using the same P.O. Box to receive payments (or whether the new provider has simply switched names and continues to fraudulently bill). To date, in the state of California alone, WellPoint has stopped over 239 bogus DME providers before they were able to submit fraudulent claims to the company.

A great example of the proactive work of the SIU in identifying bogus providers and also collaborating with our public partners at CMS and DOJ involves identifying and deterring health care fraud in the Medicare Advantage program. After a tip from one of our Medicare Advantage members who received an EOB for thousands of dollars of services he did not receive from an unknown provider, WellPoint commenced an investigation that led to the discovery of what appeared to be a large medical identity theft scheme perpetrated by an organized crime group. Further investigation of this organization resulted in discovery of bogus providers who were submitting fraudulent Medicare Advantage claims. In many cases, the perpetrators had stolen the provider identification numbers from local physicians, and utilized stolen Medicare Advantage identification members' numbers. Once this information was in hand, they began a deliberate and well-executed conspiracy to defraud our Medicare Advantage program. Our investigation revealed that claims paid from bogus providers were often for billings of a high volume of expensive infusion therapy (cancer and HIV-related) treatments for unknown conditions and from unknown providers. The claim profile of these providers exhibited the characteristics of having invalid contact information (but including identification information from legitimate doctors to make them appear genuine), as well as irregular banking methods to cash payment checks.

Our SIU worked closely with claims operations areas to develop a proactive program to assist in identifying any provider fitting the same claim and provider profile as the bogus providers. The proactive process involves identifying any previously unknown provider billing the suspicious high dollar infusion therapy. These providers and their claims are immediately pended in the system and submitted to the SIU for review. Additionally, with respect to providers already in the claims systems with the same billing and provider profile, an edit process was inserted in the claims system to pend and review claims similar to those used by the bogus providers.

As a result of the investigation, in 2011 SIU identified 36 bogus providers who engaged in this scheme. Due to the proactive work of SIU, $33 million dollars of fraudulent claims were stopped during the claims adjudication process, or newly issued checks to the perpetrators were stopped before they were negotiated. The total amount in savings to the Medicare Advantage program was $33,748,292.94.

7. Review of Emerging Technologies

Every week WellPoint reviews newly emerging technologies to determine whether providers are inappropriately billing for services, devices or medications that are currently experimental or investigational. WellPoint performs data mining to detect the wrongful billing of experimental medications and medical services by the use of codes to make the services appear legitimate. In order to receive health insurance reimbursement, some providers bill for experimental/investigational devices, pharmaceuticals, or procedures by using a set of medical codes that they know the health insurer will pay. It is fairly easy to spot the billing of new technologies as providers typically advertise them on their websites.

One such fraudulently billed new technology was an experimental back treatment known as VAX-D, a mechanical table used to stretch a patient's spine. WellPoint considers VAX-D to be investigational and not medically necessary, and clearly communicated to health care providers that it did not cover the procedure. From 2004 to 2006, WellPoint's SIU began investigating an anesthesiologist who was providing primarily physical medicine procedures at a privately-owned physician's office. Through patient interviews, the SIU determined that the office was providing back treatments using a VAX-D machine, and recovered a document that identified suggested billing codes to use for VAX-D which deviated from the specific HCPCS[4] code for VAX-D. Most insurers, including WellPoint plans, do not pay on the appropriate HCPCS code for VAX-D, but insurers do pay on the suggested codes.

WellPoint referred its investigation to the FBI in 2005 and worked closely with the federal government, which led to seven indictments, five guilty pleas, two convictions after trial, and a restitution order of approximately $4 million. Two of the providers went to trial. Evidence at trial showed that the clinic at which the two chiropractors worked billed one of WellPoint's affiliated health plans for more than $3 million relating to the VAX-D procedure from 2001 through 2005. These defendants were convicted of lying to our affiliated health plan as to the procedures the clinic was performing in order to get paid for this non-covered procedure. Specifically, instead of using the specific billing code assigned to VAX-D, the clinic used a different code that pertained to surgical nerve decompression procedures. The indictment charged that the defendants used that code because they knew our affiliated health plan would pay for it, but would not pay for VAX-D. The proof at trial included testimony from the

[4] "HCPCS" stands for Healthcare Common Procedure Coding System.

defendants' former employees, several of whom were explicitly instructed by the two chiropractors to not refer to the procedure as VAX-D when speaking to insurers, and to white-out references in documents to VAX-D because the defendants told the employees that insurers do not cover VAX-D.

WellPoint has recovered several million dollars (and expects to recover more through restitution), and the seven main perpetrators of the crime have either pled guilty or been convicted and sentenced.[5]

The VAX-D investigation has benefited WellPoint members by protecting healthcare dollars that would be lost to purveyors of a device that, to date, has not proven to be clinically effective in treating back pain. As such, the investigation has been a valuable tool to uphold the integrity of the health care system. Other plans have also benefited, as WellPoint has shared its findings with many commercial insurers. Other plans can pursue similar investigations and, given the success of the United States Attorney's Office in prosecuting the case, likely involve law enforcement and prosecutorial agencies.

[5] http://www.justice.gov/usao/gan/press/2008/07-29-08b.pdf

**Recommendations:**

Based on our experience in combating health care fraud and abuse, WellPoint offers the following recommendations to enhance future efforts throughout all sectors of health care:

- **Medicare Restricted Recipient Program**

WellPoint is supportive of giving CMS the authority to establish a restricted recipient program in Medicare Part D for those beneficiaries displaying a pattern of misutilization. WellPoint systematically reports beneficiary-specific concerns— based on objective, standardized metrics—to CMS or to Medicare Drug Integrity Contractors (MEDIC) for appropriate action against the individual beneficiary. To ensure members' safety, WellPoint believes that plans should not implement policies of denying a prescription fill even in cases of suspected overutilization. From a health plan perspective, we would want to work with the prescribing physician and/or refer the case to CMS or its delegate. WellPoint asks that CMS be responsible for taking any enforcement action once members suspected of misuse or overutilization have been identified by the plan sponsor. Once sufficient due diligence has been conducted by CMS or its delegate to demonstrate abuse, or upon recommendation of the provider, the member can be placed in the restricted recipient program which the plan sponsors manage pursuant to clear regulatory protocols.

- **Dual Eligible Beneficiaries**

Through our experience in providing health care coverage through both our Medicaid state-sponsored programs and Federal programs, we have observed that a large portion of the opioid and controlled substance abuses in the Part D program occur among the dual eligible population – beneficiaries eligible for both Medicare and Medicaid and often under 65 years of age. In calendar year 2011 alone, WellPoint's SIU unit tracked 34 investigations of Medicare Part D beneficiaries under the age of 65. Under current law, dual-eligible beneficiaries are allowed to change plans on a month to month basis, which permits drug seekers to switch programs frequently in order to avoid detection and escape program edits or substance abuse programs.

WellPoint recommends that dual eligible beneficiaries with evidence of drug-seeking behavior should be locked into one managed care plan, rather than continue to be allowed to switch plans on a monthly basis to evade detection.

- **Improved Partnerships**

WellPoint supports better coordination and cooperation among CMS, DOJ, and all stakeholders. Right now there is little collaboration between the agencies and the health plans that oftentimes have the information, experience and expertise necessary for preventing and fighting fraud and abuse. In order to be truly effective throughout the health care system, both public and private sectors should be working together to share successful anti-fraud practices, effective methodologies and information about ongoing fraud investigations. For example, while health plans currently share information with the MEDIC, we are rarely informed of the ultimate result, and information collected by the agency is rarely shared with the private payers. However, we are excited by the recent creation of the Healthcare Fraud Prevention Partnership, a voluntary partnership composed of both the public and private sector for the purposes of reducing the prevalence of health care fraud. WellPoint is an active participant, and I serve on the Data Analysis and Review Committee. It is our hope that the work of the Partnership will lead to successful public/private collaboration in the prevention and detection of health care fraud.

- **Encourage Fraud Prevention in Private Health Insurance Programs**

Experience has proven in both private and public program fraud investigations that fraud prevention is much more effective and cost-effective than pursuing "pay and chase" type fraud investigations. "Pay and chase" investigations recoup only about 20 cents on the dollar, while fraud prevention investigations result in dollar-for-dollar savings by avoiding improper payments. Moreover, fraud prevention investigations often remove fraudulent and harmful providers from the healthcare system before they can do more damage to public and private healthcare programs and their members. In recent years the Department of Justice and HHS have adopted successful fraud prevention tactics. The federal government should do everything it can to encourage fraud prevention for private health insurers, as well.

One way this can be done is to permit health insurers to lift the current restriction on health insurers' fraud programs in the Minimum Loss Ratio (MLR) calculation. All expenses for health insurer anti-fraud and abuse programs should be included as "activities that improve health care quality" in the MLR calculation, since they reduce waste in the health care system, reduce the cost of health care, and enhance patient safety by helping identify and remove providers and individuals engaging in unsafe and fraudulent practices from the health care system.

Currently the MLR final regulation merely gives insurers a limited credit – up to the amount of fraud recoveries – for fraud prevention activities. In essence, this means that insurers will have to include as administrative expenses their largest portion of antifraud expenses --

those dedicated to fraud prevention. It is truly puzzling that at a time when the federal government is accelerating its efforts to prevent fraud in Medicare and Medicaid it has simultaneously issued a regulation that will serve to discourage health insurers' fraud prevention efforts. Ironically, eliminating antifraud programs will tend to increase MLR percentages because claims will be higher, but an increased MLR will be at the expense of patient safety, quality of care, and controlling health care costs, which are the very goals of the Affordable Care Act.

If private health insurers are discouraged from keeping their anti-fraud programs in place at the same time that public program anti-fraud efforts are increasing, federal law enforcement will lose a valuable source of information and tips about providers and recipients who may also be engaging in defrauding public programs. These considerations will also be crucial as the Centers for Medicare and Medicaid Services (CMS) codifies and implements the ACA's MLR for Medicare Advantage.

***

In conclusion, I would like to thank the Committee for the opportunity to testify today on behalf of WellPoint on this critical issue, and pledge our support in any efforts to make the health care system financially viable and safer for our members.

**WellPoint's Successful Fraud Prevention Programs**

Our goal at WellPoint is to prevent health care fraud and abuse for the benefit of our members' health, as well as for the health care system as a whole. In order to meet this goal, WellPoint has developed a number of different types of programs to identify and prevent health care fraud and abuse:

- Controlled Substance Utilization Monitoring (CSUM) Program
- Medicaid Restricted Recipient Program
- Pre-pay provider review program
- Predictive modeling program
- Bogus providers
- Review of Emerging Technologies

**Recommendations:**

Based on our experience in combating health care fraud and abuse, WellPoint offers the following recommendations to enhance future efforts throughout all sectors of health care:

- Establish a restricted recipient program in Medicare Part D for those beneficiaries displaying a pattern of misutilization.
- Dual Eligible beneficiaries with evidence of drug-seeking behavior should be locked into one managed care plan, rather than continue to be allowed to switch plans on a monthly basis to evade detection.
- Better coordination and cooperation among CMS, DOJ, and all stakeholders.
- Encourage Fraud Prevention in Private Health Insurance Programs by lifting the current restriction on health insurers' fraud programs in the Minimum Loss Ratio (MLR) calculation.

Mr. PITTS. The Chair thanks the gentlelady and recognizes Mr. Saccoccio for 5 minutes for an opening statement.

## STATEMENT OF LOUIS SACCOCCIO

Mr. SACCOCCIO. Thank you. And good morning, Chairman Pitts, Ranking Member Pallone, and other distinguished members of the subcommittee. I am grateful for the opportunity this morning to discuss with you the various methods we believe can be effective in combating healthcare fraud. In my testimony today, I draw upon our organization's 27 years of experience examining, understanding, and fighting healthcare fraud.

There is no silver bullet for defeating healthcare fraud. A winning antifraud strategy for Medicare must be multifaceted and include, as outlined in my written testimony, effective information-sharing among private and public payers of health care; the application of data analytics to healthcare claims; rigorous screening of providers attempting to enter or continue in the program; and a well-trained, adequate, and multidisciplinary workforce. Also, as with prescription drug fraud and diversion, solutions specially designed to address different types of fraud must be developed.

I would like to focus on the first of these points in my oral testimony, effective antifraud information-sharing among public and private payers of health care.

Healthcare fraud does not discriminate between types of medical coverage. The same schemes used to defraud Medicare and Medicaid migrate to private insurance, and schemes perpetrated against private insurers make their way into government programs. Additionally, many private insurers and Medicare Part C and D contractors provide Medicare coverage in the States, making clear the intrinsic connection between private and public interests on this issue.

The United States spends $2.8 trillion on health care annually and generates billions of claims from well over a million healthcare service and product providers. The vast majority of these providers of services and products bill multiple payers, both private and public. For example, a healthcare provider may be billing Medicare, Medicaid, and several private health plans in which it is a network provider, and may also be billing other health plans as an out-of-network provider.

However, when analyzing this provider's claims for potential fraud and abuse, each payer is limited to the claims it receives and adjudicates and is not privy to the claims information collected by other payers. In this type of environment, those intent on committing fraud bank on the assumption that payers are not working together to collectively connect the dots and uncover the true breadth of a scheme.

And it is precisely this reason why the sharing of preventive and investigative information among payers is crucial for effectively identifying and stopping healthcare fraud. Payers, whether private or public, who limit the scope of their antifraud information to data from their own organization or agency are taking an uncoordinated and a piecemeal approach to the problem.

NHCAA was formed in 1985 precisely for the purpose of serving as a catalyst for antifraud information-sharing. My written statement provides examples of the types of information-sharing activities conducted by NHCAA.

The Department of Justice also has recognized the benefit of private-public information-sharing. For example, many U.S. attorneys offices sponsor healthcare fraud task forces that hold routine information-sharing meetings. And when invited to do so, private insurers often participate in these meetings to gather and offer investigative insight.

Despite the Justice Department's general recognition of information-sharing as an antifraud tool, many, including NHCAA, saw the need to improve and expand the cooperation and antifraud information-sharing between the private and public sectors. After more than 2 years of discussions and meetings involving several interested parties, including NHCAA, the new Health Care Fraud Prevention Partnership was formally announced on July 26th at the White House.

The Health Care Fraud Prevention Partnership represents a joint HHS and DOJ initiative, bringing together antifraud associations, private insurers, and government and law enforcement agencies. The partnership's purpose will be to exchange facts and information between the public and private sectors in order to reduce the prevalence of healthcare fraud. The partnership will also enable members to individually share successful antifraud practices and effective methodologies and strategies for detecting and preventing fraud.

NHCAA has forged collaborative relationships between the private and public sectors for nearly 3 decades, and it is from this perspective that we believe the Health Care Fraud Prevention Partnership holds great promise. Just getting under way, the partnership needs time to develop and to demonstrate it can be successful. It needs consistent high-level support if it is to realize the sorts of tangible results we believe it is capable of.

Whether undertaken through NHCAA, regional task forces and workgroups, or through the new Health Care Fraud Prevention Partnership, antifraud information-sharing and cooperation between the private and public sectors is essential to being able to detect emerging scenes and trends at the earliest time possible.

Thank you for the opportunity to testify this morning. I would be happy to answer any questions that you might have.

[The prepared statement of Mr. Saccoccio follows:]

NHCAA
National Health Care Anti-Fraud Association®

Statement of Louis Saccoccio
Chief Executive Officer
National Health Care Anti-Fraud Association

on

"Examining Options to Combat
Health Care Waste, Fraud and Abuse"

Before the
United States House of Representatives
Energy & Commerce Committee
Subcommittee on Health

November 28, 2012

NHCAA

Testimony of:
Louis Saccoccio
Chief Executive Officer
National Health Care Anti-Fraud Association

Good morning, Chairman Pitts, Ranking Member Pallone and other distinguished Members of the Subcommittee. I am Louis Saccoccio, Chief Executive Officer of the National Health Care Anti-Fraud Association (NHCAA).

NHCAA was established in 1985 and is the leading national organization focused exclusively on combating health care fraud and abuse. We are unique among associations in that we are a private-public partnership—our members comprise 90 of the nation's most prominent private health insurers representing over 300 corporate entities, along with nearly 100 federal, state and local government law enforcement and regulatory agencies that have jurisdiction over health care fraud who participate in NHCAA as law enforcement liaisons.

NHCAA's mission is straightforward: 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 and abuse. Our commitment to this mission is the same regardless of whether a patient has private health coverage through an employer or as an individual, or is a beneficiary of Medicare, Medicaid, or any other federal or state program.

I am grateful for the opportunity to discuss the problem of health care fraud and abuse with you, examining options to combat it. In my testimony today, I draw upon our organization's twenty-seven years of experience examining, understanding and fighting health care fraud.

On a national level, fraud hampers our health care system and undermines our nation's economy. On an individual level, no one is left untouched by health care fraud; it is a serious and costly problem that affects every patient and every taxpayer across our nation. The extent of financial losses due to health care fraud in the United States, while not entirely known, is estimated to range in the tens of billions of dollars or more. To be sure, the financial losses are considerable, but those losses are compounded by numerous instances of patient harm — unfortunate and insidious side effects of health care fraud that impact patient safety and diminish the quality of our medical care. Health care fraud is not just a financial crime, and it is certainly not victimless.

Health care fraud takes many forms and is a serious problem regardless of the mode of health care delivery. Similarly, anti-fraud efforts must be multi-faceted, as there is no single solution to this problem. In my testimony today I will focus on the following five topics which NHCAA believes are critical for successfully combating health care fraud.

- First, the importance of anti-fraud information sharing and cooperation among all payers of health care, including the sharing of information between private insurers and public programs.

- Second, the critical and growing role of data analytics and predictive modeling in being able to detect fraud and potentially prevent precious health care dollars from being lost to fraud.
- Third, the importance of employing rigorous provider screening as a means for ensuring that only legitimate providers are able to submit claims for payment.
- Fourth, some of the innovative methods being applied with success to address a problem of growing concern for private insurers and public programs — prescription drug fraud and drug diversion.
- Finally, the importance of maintaining an anti-fraud workforce that has the skills and experience necessary to meet current and future health care fraud challenges.

## I. Cooperation and information exchange between public and private payers of health care is critical to the success of anti-fraud efforts and should be encouraged and enabled.

Health care fraud does not discriminate between types of medical coverage. The same schemes used to defraud Medicare and Medicaid migrate to private insurance, and schemes perpetrated against private insurers make their way into government programs. Additionally, many private insurers are Medicare Parts C and D contractors or provide Medicaid coverage in the states, making clear the intrinsic connection between private and public interests on this issue.

The United States spends $2.8[1] trillion dollars on health care annually and generates billions of claims from millions of health care service and product providers. The vast majority of these providers of services and products bill multiple payers, both private and public. For example, a health care provider may be billing Medicare, Medicaid, and several private health plans in which it is a network provider, and may also be billing other health plans as an out-of-network provider. However, when analyzing this provider's claims for potential fraud or abuse, each payer is limited to the claims it receives and adjudicates and is not privy to claims information collected by other payers. There is no single repository of all health care claims similar to what exists for property and casualty insurance claims.[2] The complexity and size of the health care system, along with understandable concerns for patient privacy, likely make such a database impracticable. Nevertheless, the absence of such a tool limits the effectiveness with which health claims (housed in the discrete databases of individual payers), can be analyzed to uncover potential emerging fraud schemes and trends.

In this environment, fraudsters bank on the assumption that payers are not working together to collectively connect the dots and uncover the true breadth of a scheme. And it is precisely this reason why the sharing of preventive and investigative information among payers is crucial for successfully identifying and stopping health care fraud. Payers, whether private or public, who limit the scope of their anti-fraud information to data from their own organization or agency are taking an uncoordinated and piecemeal approach to the problem.

[1] National Health Expenditure Projections 2011-2021, Centers for Medicare and Medicaid Services, Office of the Actuary. http://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/Downloads/Proj2011PDF.pdf

[2] See https://claimsearch.iso.com

The value of information sharing in health care fraud investigations cannot be overstated. Our experience as a champion of this concept for the last twenty-seven years has taught us that anti-fraud information sharing is effective in combating health care fraud.

For example, NHCAA hosts several anti-fraud information-sharing meetings each year during which private health plans and representatives of the FBI, the Investigations Division of the Office of the Inspector General for the Department of Health and Human Services (HHS-OIG-OI), State Medicaid Fraud Control Units, the Centers for Medicare and Medicaid Services (CMS), TRICARE, and other federal and state agencies come together to share information about emerging fraud schemes and trends. Other information sharing methods employed by NHCAA include fraud alerts, NHCAA's SIRIS database of health care fraud investigations, and our Request for Investigation Assistance (RIA) process which allows government agents to easily query private health insurers regarding their financial exposure in active health care fraud cases as a means to bolster developing investigations. NHCAA private-public anti-fraud information sharing works, and routinely pays dividends for our members.

The Department of Justice (DOJ) also has recognized the benefit of private-public information sharing. For example, many U.S. Attorney Offices sponsor health care fraud task forces that hold routine information-sharing meetings, and when invited to do so, private insurers often participate in these meetings to gather and offer investigative insight. In fact, eighty-nine percent of respondents to NHCAA's 2011 Anti-Fraud Management Survey[3] (a biennial survey of its private-sector members that aims to assess the structure, staffing, funding, operations and results of health insurer investigative units) report that they share case information at law enforcement-sponsored health care fraud task force meetings.

Additionally, DOJ developed guidelines for the operation of the Health Care Fraud & Abuse Control Program (HCFAC) established by HIPAA which provide a strong basis for information sharing. The "Statement of Principles for the Sharing of Health Care Fraud Information between the Department of Justice and Private Health Plans" recognizes the importance of a coordinated program, bringing together both the public and private sectors in the organized fight against health care fraud.[4]

Despite DOJ's recognition of information sharing as an anti-fraud tool, many, including NHCAA, saw the need to improve and expand the cooperation and anti-fraud information sharing between the private and public sectors. The need for this expansion was highlighted at the National Health Care Fraud Prevention Summit hosted by DOJ and HHS in January, 2010, in which NHCAA and numerous private insurers participated. This summit set into motion a determined and steady effort to develop and establish a more formalized partnership between government agencies and private sector health insurers. It was envisioned that such a partnership would facilitate anti-fraud information exchange as a means to fight health care fraud. After

[3] The National Health Care Anti-Fraud Association, The NHCAA Anti-Fraud Management Survey for Calendar Year 2011 (Washington, DC, NHCAA, July 2012) p. 44.

[4] See http://www.usdoj.gov/ag/readingroom/hcarefraud2.htm.

more than two years of discussions and meetings involving several interested parties, including NHCAA, the new Healthcare Fraud Prevention Partnership (HFPP) was formally announced on July 26, 2012 at a White House event.

The HFPP represents a joint HHS and DOJ initiative bringing together anti-fraud associations, private insurers, and government and law enforcement agencies. The HFPP charter states that: "The Partnership's purpose will be to exchange facts and information between the public and private sectors in order to reduce the prevalence of health care fraud. The Partnership will also enable members to individually share successful anti-fraud practices and effective methodologies and strategies for detecting and preventing health care fraud." The HFPP principles include:

- Sharing facts and information on data analytics and trend analysis,
- Sharing facts and information on best practices and novel, effective methodologies,
- Support equitable information exchange,
- Balance the interests of all stakeholders,
- Make results available to support their internal anti-fraud initiative, and
- Sharing individual input on expansion to include other entities that participate in detecting and preventing healthcare fraud.

The collective input of all the parties involved in the development of the HFPP has resulted in a thoughtful and sound organizational structure. An Executive Board provides the strategic direction for the initiative, and two committees will focus on different aspects of the information exchange process:

- The Data Analysis and Review Committee (DARC), which focuses on the operational aspects of data analysis and review and the management of the data analytics, and
- The Information Sharing Committee (ISC), which focuses on sharing the aggregated results and the best practices of the participants both internal to the partnership and to external stakeholders.

Both committees are working to develop short and long-term goals. One of the goals being discussed is the ability of the DARC to collect data from participants to be analyzed by a trusted-third party with the results of the analysis being shared as decided by the ISC. The ISC is looking at its interface with law enforcement, and hopes to make use of the numerous U.S. Attorney-based task forces and work groups around the country to foster greater information sharing and cooperation. NHCAA also has urged that DOJ, FBI and HHS-OIG-IG to provide detailed guidance to their agents in the field regarding the importance of information sharing and the specific criteria for sharing information with private health insurers.

NHCAA has fostered collaborative relationships between the private and public sectors for nearly three decades and it is from this perspective that we believe the HFPP holds great promise. Just getting underway, the HFPP needs time to develop and to demonstrate that it can be successful. It needs consistent, high-level support if it is to realize the sorts of tangible results we believe it is capable of.

Whether undertaken through NHCAA, regional task forces and work groups, or through the new HFPP, anti-fraud information sharing and cooperation between the private and public sectors is essential to being able to detect emerging schemes and trends at the earliest possible time. Health care payers cannot work in isolation and expect to successfully detect and prevent health care fraud.

**II. There should be continued support for the critical and growing role of data analytics and predictive modeling for health care fraud detection.**

The United States health care system currently spends $2.8 trillion dollars and generates billions of claims every year from millions of health care service and product providers. Medicare alone, representing nearly 50 million beneficiaries, pays over 4.4 million claims each working day to 1.5 million providers. Our nation's health care system hinges upon a staggering amount of data and countless health care claim adjudication systems.

Given the diversity of providers and payers and the complexity of the health care system — as well as the sheer volume of activity — the challenge of preventing fraud is enormous. Clearly, the only way to realistically deal with this complexity is to apply cutting-edge analytic techniques to the data to detect risks and emerging fraud trends.

It is much more cost effective to detect and prevent fraud prior to paying a fraudulent claim than to investigate and prosecute it after the fact. The "pay and chase" model of combating health care fraud, while necessary in certain cases, is no longer tenable as the primary method of fighting this crime. The Centers for Medicare and Medicaid Services (CMS) has signaled — through testimony, resource allocation and action — that it recognizes this and is dedicating significant resources to this operational shift to prepayment anti-fraud efforts, including the application of predictive modeling to Medicare fee-for-service claims through its Fraud Prevention System.

As a precursor to efforts currently underway, Congress demonstrated its recognition of the promise that predictive modeling techniques hold for combating health care fraud by passing the Small Business Jobs and Credit Act of 2010. Establishing predictive analytics technologies requirements for the Medicare fee-for-service program, the Act directs the U.S. Department of Health and Human Services (HHS) Secretary to use predictive modeling and other analytical technologies to identify improper claims for reimbursement and prevent their payment. Clearly, one of Medicare's strengths in terms of fraud detection is the enormous amount of data the program generates and collects. We believe that applying predictive modeling to that data could yield very powerful, game-changing results.

CMS launched its Fraud Prevention System (FPS) employing predictive modeling on July 1, 2011. The technology used is similar to that used by credit card companies and financial institutions to detect and prevent fraud. The system, which is being used by CMS and its program integrity contractors, analyzes Medicare claims data applying models of fraudulent behavior. This analysis results in automatic alerts on specific claims and providers. These alerts are, in turn, prioritized for program integrity analysts to review and investigate.

NHCAA has reviewed the recently released Government Accountability Office (GAO) report "Medicare Fraud Prevention: CMS Has Implemented a Predictive Analytics System, but Needs to Define Measures to Determine Its Effectiveness." Essentially a report card on the FPS system, the study reasonably recommends that CMS develop schedules for completing integration of the FPS with existing systems, define and report to Congress quantifiable benefits and measurable performance targets and milestones, and conduct a post-implementation review of FPS.

It is understandable that many are anxious to see immediate, positive results from the investments already made in adopting predictive modeling and analysis. On that point, NHCAA would encourage patience regarding the use of predictive modeling and data analysis for combating fraud. It will take time to effectively refine and adjust the models for such a large and complex system as Medicare in order to realize the full potential that these powerful technologies offer. Despite the challenges, this is a path that both Congress and CMS recognize has to be followed, and NHCAA strongly support this effort.

Many private health plans also have recognized the importance of predictive analytics to help detect potential fraud. Forty percent of respondents to NHCAA's 2011 Anti-Fraud Management Survey indicated the use of some form of predictive analytics in its anti-fraud work. It is important to note that predictive analytics is an important tool in the detection of fraud, but it is not a panacea. Predictive analytics can generate leads for further inquiry and can help form the basis for the suspension of payments, but it has not been used as the sole basis for the suspension of payments by private health insurers without additional follow-up and corroboration.

## III. The importance of employing rigorous provider screening.

From an anti-fraud perspective, one long-held criticism of the Medicare program has been the relative ease with which providers could gain access to the program and begin billing with little more required of them than completing and submitting the necessary paperwork. Of course, with a program that serves nearly 50 million Americans, it is important to ensure that there is acceptable access to health care to meet the needs of beneficiaries. The vast majority of health care providers are legitimate and honest, and follow the rules prescribed by the Medicare program. No one has an interest in burdening honest providers to the extent that they are dissuaded from participating in the program. These underlying considerations have for all intents and purposes culminated to establish Medicare as a program that has traditionally enabled "any willing provider" to participate.

However, to the extent that an individual or entity looks to enter the Medicare system to commit fraud, inadequate provider screening represents the Achilles' heel of program integrity. Encouragingly though, improved provider screening also may serve as our best opportunity for significant fraud-fighting "wins" under Medicare since it addresses fraud at the provider entry point. The challenge is implementing provider screening reforms that achieve the goal of cutting down on fraud while not impacting beneficiary access to care or unnecessarily encumbering legitimate providers who wish to serve the Medicare population.

The Affordable Care Act (ACA) laid the groundwork for additional and enhanced screening of providers who participate or seek to participate in Medicare and Medicaid. Section 6401 of the ACA directs the Secretary of the Department of Health and Human Services to determine "levels" of provider screening according to "the risk of fraud, waste, and abuse...with respect to the category of provider of medical or other items or services or supplier." The Secretary is authorized also to impose additional burdens where there are more significant fraud concerns and impose a temporary moratorium on the enrollment of new providers of services and suppliers under Medicare, Medicaid and the CHIP program when necessary to prevent or combat fraud, waste or abuse.

On February 2, 2011, the final rule was published that details the new provider screening requirements envisioned in the law. The rule became effective March 25, 2011, and designates categories of providers and suppliers that are subject to varying screening procedures based on the risk presented by the category of provider. Three levels of screening and associated risk were established—limited, moderate and high—with each provider/supplier category assigned to a screening level. The following are the types of screenings delineated in the rule for Medicare:

- Verification of any provider/supplier-specific requirements established by Medicare;
- Conducting of license verifications (may include licensure checks across states);

- Database checks (SSN, NPI, NPDB licensure, OIG exclusions, tax ID, tax delinquency, death);
- Unscheduled or unannounced site visits; and
- Fingerprint-based criminal history record check of law enforcement repositories.

Building upon the new provider screening requirements enabled by the ACA and the subsequent rule, in December 2011, CMS began implementing a new Automated Provider Screening (APS) system that automates the validation of provider and supplier enrollment application information, drawing upon public and private sources. Information verification, including licensure status, is automatic and continuous. The APS replaces time- and resource-intensive manual review of provider enrollment applications, thus reducing application processing time. It is also intended to assess the individual level of risk each provider and supplier presents to the Medicare program. It is useful to note that the APS system is not yet integrated with CMS's Fraud Prevention System, but it will be. This integration, according to the GAO, should "enable the Fraud Prevention System to risk-score providers based on certain public records."[5]

NHCAA supports the reforms made to the Medicare provider screening process in the last year. In our view, they represent common sense steps that are capable of being adjusted as the discerned risks change over time. To protect our investment in the program, it is important that Medicare enrolls only qualified providers and suppliers who meet and maintain compliance with

[5] See http://www.gao.gov/assets/650/649537.pdf p. 25.

the program's participation requirements. The screening processes now in place do a good deal in the service of that goal.

IV. **Special emphasis on prescription drug fraud and drug diversion.**

Our resources to combat health care fraud, waste and abuse are finite. Difficult decisions must be made about how best to allocate those resources. Based on projected increases in spending for prescription drugs, the expansion of health coverage envisioned by the Affordable Care Act, and our experience and insight about health care fraud trends, NHCAA believes prescription drug fraud will continue to grow as a segment of the health care fraud problem and, therefore, deserves special consideration.

National Health Expenditure Data reveal that in 2010, $259 billion dollars were spent on prescription drugs and by 2021, that spending is projected to nearly double, reaching $483 billion.[6] It is notable that in 2014 an estimated 18 million Americans will become newly insured under Medicaid and through Exchange plans,[7] significantly influencing the 8.8 percent annual increase projected for prescription drug spending in that year alone.[8] Private and public insurers underwrite 80 percent of all spending on prescription drugs in the U.S., while consumers pay

[6] http://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/Downloads/Proj2011PDF.pdf

[7] http://www.cbo.gov/budget/factsheets/2011b/HealthInsuranceProvisions.pdf

[8] http://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/Downloads/Proj2011PDF.pdf, Table 11

roughly just one-fifth of the cost.[9] This means insurers and public programs shoulder the bulk of exposure, risk and ultimately financial losses resulting from drug diversion and other prescription drug fraud schemes.

No insurer or public health care program is immune. Findings from a Government Accountability Office (GAO) report issued in September of last year titled "Medicare Part D: Instances of Questionable Access to Prescription Drugs"[10] describe how the Medicare Part D prescription drug program is vulnerable to prescription drug abuse. Acknowledging this vulnerability, CMS issued a memorandum to Part D sponsors in late September 2011 seeking input on how to improve drug utilization review controls under the program[11]. This past April CMS published its Final Call Letter[12] that included a section on improving drug utilization review controls in Part D that delineates several improvements to formulary management processes that should be implemented by sponsors in order to comply with drug utilization management requirements. The letter lays out a minimum compliance standard with respect to overutilization of opioids and explains that if the drug utilization review levels described do not prove effective at establishing medical necessity, sponsors may implement beneficiary-level point of service restrictions under certain conditions.

[9] http://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/Downloads/Proj2011PDF.pdf, Table 11

[10] See http://www.gao.gov/products/GAO-11-699

[11] See http://www.cms.gov/Medicare/Prescription-Drug-Coverage/PrescriptionDrugCovContra/Downloads/Improving-DUR-Memo-Controls.pdf

[12] See http://www.cms.gov/Medicare/Health-Plans/MedicareAdvtgSpecRateStats/Downloads/Announcement2013.pdf, p 131

Health care fraud is most often discussed in terms of financial loss, but it can also be the catalyst for patient harm and even death. The nature of prescription drug fraud, with its risk of overdoses, unsafe drug interactions, and the taking of unnecessary and often addictive medication is particularly prone to lead to patient harm. The Office of National Drug Control Policy calls prescription drug abuse "the Nation's fastest-growing drug problem,"[13] and the Centers for Disease Control and Prevention classifies prescription drug abuse as an epidemic. The 2011 National Drug Threat Assessment report produced by the Department of Justice National Intelligence Center says that the abuse of controlled prescription drugs "constitutes a problem second only to the abuse of marijuana in scope and pervasiveness in the United States."[14] Of course, prescription drug abuse in itself does not necessarily indicate fraud. Abuse (resulting in overdoses and deaths) can certainly occur in situations where the prescription drugs were legitimately obtained for legitimate purposes. Nevertheless, fraud likely plays a role in many instances.

The practice frequently referred to as "doctor shopping" whereby individuals obtain prescriptions for frequently abused drugs from multiple prescribers and then fill them at different pharmacies, has garnered significant attention in recent years. This represents but one form of a broader prescription drug fraud scheme commonly referred to as drug diversion. With recent focus on doctor shopping by decision-makers and the media, it is important to acknowledge that prescription drug fraud and diversion can actually take many forms and be extremely complex. For example, doctor shopping isn't always perpetrated by beneficiaries alone. Sometimes

[13] See http://www.whitehouse.gov/ondcp/prescription-drug-abuse

[14] See http://www.justice.gov/ndic/pubs44/44849/44849p.pdf

prescribing physicians, as well as pharmacists, are complicit or even drivers in the scheme. Patients also may be involved with the forging of prescriptions using prescription pads that have been stolen from legitimate physicians. Other schemes include unscrupulous physicians selling prescriptions to abusers or street dealers. Still another has perpetrators taking part in a criminal enterprise directed at reselling drugs in high volume (and for large profits) on the street. Regardless of the form drug diversion takes there is usually a common thread—the drugs are obtained and paid for by filing false insurance claims.

Notably, the money lost to prescription drug fraud through payment of bogus pharmacy claims is only a part of the financial impact of this problem. In the process of obtaining a prescription, a patient typically will generate claims for related medical services. Insurers and government health care programs often find that they have paid not just for unnecessary medications but also for related emergency room visits, in-patient hospital stays, visits to physician offices and clinics, diagnostic testing and rehabilitation—all based on phantom injuries, illnesses and conditions feigned in order to obtain a prescription. Then there are the additional costs associated with treating the addictions and overdoses arising from this behavior.

To offer some perspective, a 2007 study produced by the Coalition Against Insurance Fraud titled "Prescription for Peril," states that insurer WellPoint, Inc. found that it "paid $41 in related medical claims for every $1 it paid in narcotic prescriptions for suspected doctor-shopper plan members."[15] That is an astonishing ratio and a significant waste of medical resources. And a

[15] http://www.insurancefraud.org/downloads/drugDiversion.pdf

survey conducted by the Substance Abuse and Mental Health Services Administration's Office of Applied Studies (SAMHSA/OAS) titled "The Drug Abuse Warning Network (DAWN) Report," finds: "The estimated number of emergency department (ED) visits involving nonmedical use of narcotic pain relievers rose from 144,644 in 2004 to 305,885 in 2008, an increase of 111 percent."[16] While we can't assume that all of those emergency room visits were the result of prescription drug fraud and abuse, we can reasonably assume that many of them were and therefore the cost of some of those visits constitute fraud losses.

NHCAA insurer members have recognized doctor shopping as a fraud trend over the last several years and their anti-fraud efforts regularly identify dangerous prescription drug abuse by patients. Most often, it's the insurer that is best able to connect the dots and identify overprescribing by physicians and prescription drug abuse by patients based on review of claims data. Many insurers use pharmacy benefit managers (PBMs) to carry out pharmacy functions, tasking them also with claims integrity. However, because a PBM's responsibility is typically limited to prescription claims it is often unable to detect the larger scheme that takes into account the related medical services.

In order to meet the growing threat of prescription drug fraud, several NHCAA members as well as some state Medicaid programs are devoting significantly increased resources to the problem, developing policies to quickly detect suspected doctor shopping and drug diversion, and implementing programs to stop it.

[16] http://oas.samhsa.gov/2k10/dawn016/opioided.htm

To try and identify possible doctor shopping many insurers run data mining reports that regularly search across claims data applying certain criteria in order to identify enrollees whose prescription drug claims history meet thresholds that may indicate abuse. For example, one insurer uses what it calls a 333 report which identifies enrollees who in the last year have gone to three or more prescribing doctors, have filled prescriptions at three or more pharmacies and have received three or more prescriptions for schedule III or IV controlled substances. Fraud investigators use the report to launch a more in-depth examination of the claims history to try and identify and confirm doctor shopping. Some insurers take the list of members identified via data mining reports to serve as the basis for monthly mailings to prescribing doctors, aimed at making them aware when one of their patients has been going to several providers seeking similar prescription drugs.

When an insurer determines that doctor shopping has occurred the member may be required to participate in a restricted recipient program or "lock-in" program whereby the member is limited to filling prescriptions at one pharmacy or limited to receiving prescriptions from just one doctor. Some insurers choose to employ anti-fraud staff members that are dedicated exclusively to investigating prescription drug fraud. In fact, one national health insurer that is a NHCAA member devotes a quarter of its anti-fraud investigative manpower to prescription drug fraud.

Many of the programs that private insurers have put in place to combat prescription drug fraud — things like running overutilization reports, letter campaigns making prescribers aware of possible drug-seeking behavior and restricted recipient programs — have been quite successful. Other promising tools include utilizing geo-mapping technologies to identify members who appear to be traveling long distances to obtain controlled substances from physicians or pharmacies, identifying prescribers who are writing prescriptions that fall outside their scope of specialty, and looking closely at large concentrations of claims coming from a single pharmacy.

Prescription drug fraud is a serious issue with severe patient harm risks. In meeting their obligations to provide coverage and make prompt claims payments, health insurers, including government programs and private health care payers, often pay for the unnecessary prescription drugs as well as the related medical services. Insurers are devoting increased attention and resources to this problem, devising new and innovative ways to detect possible drug diversion and taking appropriate steps to stop it, while also trying to help patients in need of intervention and treatment. We commend these actions and encourage CMS to make rooting out fraud in the Medicare Part D program a priority.

## V. Ensure a skilled and sufficient workforce of health care anti-fraud professionals with the skills and experience necessary to meet current and future health care fraud challenges.

Individuals who work to prevent, detect and investigate health care fraud, waste and abuse in our government programs have a challenging task that demands a wide set of specialized skills. Health care fraud is a complex crime that can manifest itself in countless ways. There are many variables at play. The sheer volume of health care claims makes fraud detection a challenge. Add to that the fact that fraud can conceivably be committed by anyone, and that those committing fraud have the full range of medical conditions, diagnoses, treatments and patients on which to base false claims. Plus, detecting health care fraud often requires the application and knowledge of medical and clinical best practices, terminology and arcane coding systems including CPT, CDT and HCPCS codes, DRGs, ICD-9 codes, and the forthcoming ICD-10 codes. The unique and intricate structures of our varied and numerous government health care programs add to the difficulty of effectively combating fraud and abuse.

Fraud schemes and trends often emerge from particular medical specialty areas or involve very specific treatments, diagnoses or procedures, but those schemes constantly change, develop, shift, migrate and morph. And geography plays a prominent role too. It is typical to see a fraud scheme established in one geographic region move to a different region once the payer and law enforcement communities in the original region react to the scheme.

With its complexity, our health care system can be susceptible to creative, nimble and aggressive perpetrators who have a knack for identifying weaknesses. This fact demands that we employ fraud fighting techniques that are equally creative, nimble and aggressive. To that end, investments need to continually be made to educate and train the anti-fraud workforce on the front lines to ensure that it is knowledgeable about the latest trends and schemes, as well as the newest tools and techniques for fraud detection and prevention.

Since our founding, NHCAA has provided the professional health care anti-fraud field with superior education and training opportunities, developing and delivering unique training programs specifically designed to advance the professionalism and knowledge of the individuals, both private and public, responsible for the fight against health care fraud. Our Annual Training Conference is the largest education event we host each year, attracting more than 1,200 investigative professionals, a large percentage of whom are public sector employees. In addition, NHCAA offers the Accredited Health Care Anti-Fraud Investigator (AHFI) designation. Achieving an AHFI is widely considered the gold standard of professionalism in health care fraud investigation.

Along with education, ensuring adequate staffing levels is also critically important. There is currently much attention given to predictive modeling and prepayment analytics, and with good reason. However, the need for "boots on the ground" is as great as it has ever been. Technology professionals and data analysts will be in increasing demand as the use of prepayment technologies grows. And the leads and information developed by data analytics will continue to require, in many instances, skilled investigators and medical record reviewers with clinical backgrounds available to act on the information. It is important that the anti-fraud units responsible for ensuring the integrity of our federal health care programs are staffed sufficiently to meet the challenge that fraud and abuse presents. As we focus on the promise of technology, we mustn't overlook the vital need for smart, analytical, insightful, and committed fraud-fighting professionals.

We must maintain a multi-prong approach to fighting health care fraud that strikes a balance between technological resources and human resources. So as we continue to extol the promise of cutting-edge technologies for combating health care fraud, waste and abuse, we must also champion the continued investment in human capital. We recommend that in its allocation of funding for anti-fraud efforts in Medicare and Medicaid, Congress recognizes the necessity of building a workforce with the numbers, depth, specialization and skill necessary to be successful.

**Conclusion**

There is no silver bullet for defeating health care fraud. A winning strategy for Medicare must be multi-faceted and include effective information sharing among private and public payers of health care, the application of data analytics to health care claims, rigorous screening of providers attempting to enter and continue in the program, and a well-trained, adequate and multi-disciplinary work force. Also, as with prescription drug fraud and diversion, solutions specially designed to address different types of fraud must be adopted.

Additionally, a winning strategy must be supported by adequate funding. When it was established through HIPAA, the National Health Care Fraud & Abuse Control Program (HCFAC) was intended to be "a far-reaching program to combat fraud and abuse in health care, including both public and private health plans."[17] After 15 years, the HCFAC program shows a

[17] See http://oig.hhs.gov/publications/docs/hcfac/hcfacreport2011.pdf, The Department of Health and Human Services and The Department of Justice Health Care Fraud and Abuse Control Program Annual Report for Fiscal Year 2011, page 3.

return on investment (ROI) of $5.10 for every $1 spent since the program began[18]. In addition, the program has returned more than $20.6 billion to the Medicare Trust Fund since its inception. Similarly, NHCAA's private-sector members consistently earn solid returns for their anti-fraud investments.

The HCFAC allocations for fiscal year 2011 totaled $608 million (including mandatory and discretionary allocations), which may seem sizeable. However, considering that nearly $1 trillion dollars is currently spent on Medicare and Medicaid ($557.8 billion spent for Medicare and $428.7 billion for Medicaid)[19], that $608 million investment is very small by comparison (representing just 0.06% of expenditures), especially in light of the demonstrated return on investment from anti-fraud spending.

Health care fraud costs taxpayers billions of dollars every year, and fighting it requires focused attention, continuous resource investment and a long-standing commitment to pursuing and adopting innovative solutions. Based on our history as a private-public partnership, NHCAA believes that a comprehensive approach to fighting fraud must include all payers, public and private, and embrace private-public solutions. Government entities, tasked with fighting fraud and safeguarding public programs, and private insurers, responsible for protecting their

[18] See https://oig.hhs.gov/publications/docs/hcfac/hcfacreport2011.pdf, p. 8.

[19] National Health Expenditure Projections 2011-2021, Centers for Medicare and Medicaid Services, Office of the Actuary. http://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/Downloads/Proj2011PDF.pdf

beneficiaries and customers, can and should work cooperatively on this critical issue of mutual interest.

Thank you for allowing me to speak to you today. I would be happy to answer any questions that you may have.

Mr. PITTS. The Chair thanks the gentleman and now recognizes Mr. Pattinson for 5 minutes for an opening statement.

## STATEMENT OF NEVILLE PATTINSON

Mr. PATTINSON. Thank you, Chairman Pitts, Ranking Member Pallone, and members of the subcommittee, for inviting me to testify on the solution to the problems for Medicare waste, fraud, and abuse. My name is Neville Pattinson, and I am the senior vice president of Gemalto. And I am here today representing the Secure ID Coalition.

Gemalto is the world's leader in digital security, with over a billion people using our products every day. We develop secure operating systems and run them on secure devices that include smart cards, banking cards, U.S. passports, electronic ID cards, and tokens.

Founded in 2005, the Secure ID Coalition is composed of companies which make smart cards and attendant technologies. We work with industry experts, public policy officials, and government agencies to promote identity solutions that both enable security and privacy protections. We are offering our industry expertise in the area of contact smart cards, which are used extensively throughout the Federal Government and around the world to protect access to both physical and logical assets as well as to protect personal information.

Our Nation's Medicare system is under attack. Medicare abuse and fraud needlessly costs American taxpayers billions of dollars every year. The Centers for Medicare and Medicaid Services estimated in 2010 over $65 billion in improper Federal payments were made through both the Medicare and Medicaid programs. An April 2012 study published in the Journal of the American Medical Association estimated that fraud and abuse cost Medicare and Medicaid as much as $98 billion in 2011. Despite these good-faith estimates, the true cost of fraud and abuse in health care remains unknown.

If we are ever to curb the fraud within the Medicare system, we need to start verifying those who are authorized to provide services, verify those who are authorized to receive benefits, and prevent those who are unauthorized from ever entering the system. Unfortunately, our current inability to address this fundamental identity and verification problem leaves the Medicare system perpetually open to ongoing exploitation. Programs to curb Medicare fraud without first resolving the identity verification problem will ultimately fail if we don't know who is a legitimate beneficiary and who is not.

In order to get to the right track, we must structure the Medicare system to prevent fraud before it happens. This will not only save taxpayers billions of dollars every year, but ensure that Medicare survives to serve Americans well into the future. The Medicare Common Access Card Act, or the Medicare CAC, H.R. 2925, introduced by Congressman Gerlach and Congressman Blumenauerand Congressman Shimkus, is an important bipartisan piece of legislation that looks to solve this problem.

In short, it calls for a pilot program to modernize the current Medicare card in order to verify both providers and beneficiaries as legitimate participants in the program. In it, five regional pilots would test upgrading the current paper Medicare card to a secure smart card, similar to those used by the DOD and all Federal employees.

The pilots would do three things. First, it would reduce the number of fraudulent transactions by eliminating ways criminals can scam Medicare. Secondly, it would create significant efficiencies within the Medicare program, providing enormous benefit to the legitimate providers and their patients. And, lastly, and some would say most importantly, it would remove the Social Security number from the front of the Medicare card, immediately protecting seniors from identity theft and fraud.

Here is how it would work. When checking out at the doctor's office, the beneficiary inserts their upgraded Medicare card into a reader and inputs their PIN code. The provider simultaneously inserts their upgraded provider card and scans perhaps their finger. This guarantees the transaction is agreed to, authenticated, and is legitimate. It has been electronically signed and encrypted and sent directly to CMS.

What enables the transaction of the high-level assurance is a secure smart card embedded into the card. Smart cards are based on established, nonproprietary, open standards widely used by the Federal Government. Additionally, government healthcare systems globally utilize smart cards. The French, German, Taiwanese healthcare systems all use similar twin card systems to eliminate fraud and increase efficiencies.

Smart cards are also widely used throughout the private sector. Financial services companies worldwide issue debit cards and credit cards to their consumers to prevent fraud and abuse. American banks will be introducing these Chip and PIN cards starting next year. But based on the savings reported by the U.K. financial services industry, the use of smart cards in that sector led to a reduction in overall fraud losses upwards of 70 percent.

Mr. Chairman, I realize I am running out of time, and I beg to continue for another minute.

Mr. PITTS. You may proceed.

Mr. PATTINSON. Thank you, sir.

While industry experts believe that Medicare CAC will be able to deliver similar results, it is entirely reasonable to assume a cost savings of at least 50 percent. At the current rate of fraud, that represents well over $30 billion a year.

We are not claiming this will eliminate fraud as we know it, nor is it a panacea. You may hear of vulnerabilities of otherwise resilient and stalwart systems. For that, our security innovations are constantly improving to solve current exploits and prevent future ones. The point is not to create an invulnerable system. That is impossible. The point is to save the Medicare system for the next generation.

Existing fraud-mitigation technologies currently used by CMS cannot do it alone. We must prevent bad actors from getting into the system to begin with. Contact smart cards are the strongest, surest, proven, and most mature technology to do that.

In conclusion, we are confident that a program such as Medicare CAC will bring value to beneficiaries, providers, and taxpayers alike. For beneficiaries, Medicare CAC ensures that their sensitive personal information, including their Social Security number, is protected by strong encryption that can only be read by an authorized Medicare CAC card reader. Providers will benefit from quicker processing of payments, increased billing accuracy, and the protection of their Medicare provider ID numbers. And taxpayers will ultimately gain the most significant benefit: the reduction in fraud, waste, and abuse within the Medicare system that can prevent the loss of tens of billions of dollars every year.

Everone in Congress wants to preserve Medicare for the next generation of beneficiaries. Medicare CAC does this without having to raise taxes, eliminate benefits, or cut reimbursements. In our opinion, it is the best outcome for all possible solutions.

Mr. Chairman, Ranking Member, and members of the subcommittee, I will be happy to answer questions that you may have. Thank you.

[The prepared statement of Mr. Pattinson follows:]

**Testimony of**
**Neville Pattinson**
**Senior Vice President**
**Gemalto, Inc.**

**On behalf of the**
**Secure ID Coalition**

**Before the**
**House Energy & Commerce Subcommittee on Health**

**Hearing on**
**Examining Options to Combat Health Care Waste, Fraud, and Abuse**

**November 28, 2012**

SECURE COALITION ID
Protecting Identity with Technology

## TABLE OF CONTENTS

**About the Secure ID Coalition:**
Founded in 2005, the Secure ID Coalition works with industry experts, public policy officials, and federal and state agency personnel to promote identity policy solutions that enable both security and privacy protections. Because of our commitment to citizen privacy rights and protections we advocate for technology solutions that enable individuals to make decision about the use of their own personal information. Members of the Secure ID Coalition subscribe to principles that include the increased deployment of secure identity solutions, as well as advise on and advocate for strong consumer privacy protections and enhanced security to reduce waste, fraud, theft and abuse. Our mission is to promote the understanding and appropriate use of smart card technology to achieve enhanced security for ID management systems while maintaining user privacy. Such ID management systems include physical and/or logical access to facilities and networks. For more information, please visit our website at www.secureIDcoalition.org.

## INTRODUCTION

Thank you Chairman Pitts, Ranking Member Pallone, and Members of the Subcommittee for inviting me to testify on solutions to the problem of Medicare fraud, waste and abuse. My name is Neville Pattinson, Senior Vice President, Gemalto, and I am here today representing the Secure ID Coalition.

**Gemalto** is the world leader in digital security with North American headquarters in Austin, TX and 2011 annual revenues of over $2.5 billion. With over 10,000 employees operating out of 74 offices and 14 Research & Development centers, we are dedicated to delivering innovative products, services, and solutions for our customers in over 40 countries. Gemalto issues more than 1.2 billion credentials per year out of our 18 production and 30 central issuance centers, which are certified to the highest security standards in the industry. To find out more about us please visit www.gemalto.com , blog.gemalto.com, or follow us on Twitter: @gemalto_NA.

Founded in 2005, the **Secure ID Coalition** is composed of companies which make smart cards and their attendant technologies. We work with industry experts, public policy officials, and federal and state agencies to promote identity policy solutions that enable both security and privacy protections.

We are here to offer our industry expertise in the area of smart cards, which are used extensively throughout the federal government and around the world to protect access to both physical and logical assets, as well as to protect personal information.

## IMPROVING MEDICARE & MEDICAID PROGRAM INTEGRITY

### *Prevention is 90 Percent of the Cure*

Our nation's Medicare and Medicaid programs are under attack. The Centers for Medicare and Medicaid Services (CMS) estimated that in 2010, over $65 billion dollars in improper federal payments were made through both the Medicare and Medicaid programs. An April 2012 study published in the Journal of the American Medical Association estimated that fraud and abuse cost Medicare and Medicaid as much as $98 billion dollars in 2011.[1] Despite these good faith estimates, the true cost of fraud and abuse in health care remains unknown; however one point is certain: the financial impact of waste, fraud and abuse threatens the very existence of the Medicare and Medicaid programs.

The reason for such a monumental waste of taxpayer funds is a systemic lack of accountability: criminals posing as durable medical equipment providers billing Medicare for products never

[1] Berwick, Donald M. and Andrew D. Hackbarth, "Eliminating Waste in US Health Care," *JAMA* 307, no. 14 (2012): 1513–6, doi:10.1001/jama.2012.362.

sold, rogue providers billing for services never rendered, and inattentive office staff billing Medicare for treatments never allowed. If fraud, waste and abuse within the Medicare and Medicaid systems are ever to be curbed, the very first place we need to start is being able to know and verify who is authorized to provide and receive these important benefits – while preventing those who are not – before the claim is ever made.

Unfortunately, our current inability to address this fundamental identity and verification problem leaves both the Medicare and Medicaid systems perpetually open to ongoing exploitation. Programs to curb Medicare and Medicaid fraud, waste and abuse without first resolving the identity verification problem will ultimately fail if we don't know who is a legitimate beneficiary or provider, and who is not.

Structuring the Medicare and Medicaid systems to prevent fraud will not only save taxpayers billions of dollars every year, but ensure that these two very important programs survive to serve Americans now and well into the future.

**Securing the Cards and Transactions**

Our recommendation is to address the problem of **identity verification** of beneficiaries, providers and suppliers as well as **securing billing transactions** in Medicare. The proposal calls for upgrading the Medicare card to secure transactions as has been done in other federal programs and other health programs across the world. Many or our recommendations are contained in the **Medicare Common Access Card Act** introduced last year in the both the House (HR.2925) and Senate (S.1551), both of which are endorsed by the American Association of Retired Persons (AARP). These bills call for an upgraded Medicare card, based on a secure smart card, to verify who is eligible to give and receive benefits as a pre-condition to the claim ever being presented to the Centers for Medicare and Medicaid Services (CMS) for payment.

Under the proposal for beneficiaries, the new smart card would securely store the Medicare account number or identifier (which today is the Social Security number) on a secure micro-controller. Providers and suppliers will also receive a new smart card, securely storing their National Provider Identity number (NPI), so that only they can use it. By requiring identity verification of providers and beneficiaries before a claim can be filed and payment processed, Medicare would easily eliminate more than fifty percent of the fraud within the current system. Smart card solutions are used throughout the Federal government as employee credentials, within the States as benefits cards, and in local hospitals and health systems to reduce errors, eliminate duplicate electronic records and to save administrative costs. For the purposes of this bill, the program outlined calls out Medicare specifically. Our industry has been discussing and promoting an upgraded Medicare card to reduce fraud, waste and abuse within the program over the past several years.

However, smart cards could easily be deployed within Medicaid. Currently, several states including Georgia, North Carolina and Virginia are considering smart cards and biometrics programs as a way to reduce fraud, waste and abuse within Medicaid. The Secure ID Coalition continues to reach-out and dialogue with a number of healthcare providers and others in the healthcare community to educate them about the potential benefits of the smart card technology solution.

## WHAT IS THE PROBLEM?

**Provider-Based Fraud and Error:**

- Phantom billing is where fraudsters or unscrupulous medical providers bill Medicare for unnecessary or unperformed procedures, medical tests, or equipment (or for equipment that is billed as new but is, in fact, used).

- NPI numbers of upstanding providers are stolen by fraudsters and criminals and used to file claims. In this case providers are unaware their Medicare account is being used for nefarious purposes.

- Durable medical equipment abuse can happen when medical equipment used in the home - like wheelchairs or oxygen tanks - are billed many times over, while in fact nothing has been delivered to an actual patient.

- Processing errors and mistakes account, in many cases, for improper payment. These payments either should not have been made or were made in an incorrect amount. Improper payments also include payments sent to the wrong recipient or payments where supporting documentation is not available.

**Patient-Based Fraud:**

- Fraudulent patient billing can occur when a patient provides his or her Medicare number to a provider in exchange for kickbacks. The provider bills Medicare for any reason and the patient is told to admit that he or she indeed received the medical treatment.

- "Card Swapping" passed-off or stolen Medicare cards are used by others to get medical care.

## WHAT IS THE SOLUTION?

**A Medicare Common Access Card**

The term "common access card" derives from the original federal government smart card program: The Department of Defense's Common Access Card (CAC). The DOD CAC was implemented in 2000 as a means of authenticating personnel with access to DOD facilities and computers. Upon full deployment, network intrusions were reduced by nearly 50% overnight. The CAC model and platform has also been rolled out across the federal government for all employees and contractors known as the Personal Identity Verification (PIV) program.

A Medicare CAC would leverage the existing government platform for secure identity credentials to modernize how information is protected within the Medicare system itself. Doing so protects the personal information of every beneficiary and puts in place a front-end prevention system to only allow authorized providers and suppliers to bill for Medicare services.

Authenticating Medicare beneficiaries and providers during an enrollment process and requiring the use of secure personalized credentials will reduce fraud by:

- Verifying beneficiaries are authorized to receive services and pharmaceuticals or equipment being prescribed;
- Verifying providers are authorized to provide those services and bill Medicare;
- Verifying suppliers, such as durable medical equipment (DME) vendors, are authorized to provide products and/or services and bill Medicare
- Preventing imposters from posing as beneficiaries or providers, thereby thwarting fraudulent transactions; and
- Verifying and coding each transaction to prevent phantom billing, processing errors and DME abuse.

Further, an upgraded Medicare card would protect beneficiary's privacy by taking their Social Security number off the front of the Medicare card, and locking it securely within the card's onboard computer chip – an important step in helping to reign in identity theft.

**Card Issuance and Use**

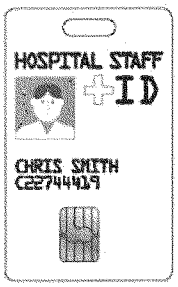
Today when a beneficiary first enrolls in the Medicare program they verify their identity with documents or certificates on record with the Social Security Administration. Under Medicare CAC the process for beneficiary enrollment would not change. After electing to receive Medicare, beneficiaries receive a new secure smart card in the mail containing their protected identification information on an embedded micro-controller. For security purposes, a unique PIN code would be mailed to the beneficiary separately. The card and PIN together authenticate the beneficiary at check-in and authorize the transaction with the provider at the point of service or check-out. This process, using a smart card with a PIN code, is known as two-factor authentication.

Medicare providers verify their identity and eligibility to provide services during an enrollment process. Currently, under the Affordable Card Act (ACA) high risk providers go through an enrollment process to verify their credentials and identity. Under the proposed Medicare CAC, each provider's identity is secured by supplying a biometric that will serve as their own unique key to their Medicare billing account. Providers receive a secure smart card which includes an embedded micro-processor that stores basic biographical information, their NPI, as well as their unique biometric key, thus binding the credential to the individual. The card and the biometric together authenticate the provider, similar to two keys used to open a safety deposit box (another type of two-factor authentication).

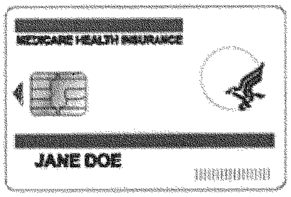
At the point of service, the transaction is authorized by both the provider and the beneficiary by creating an electronic verification between their two smart cards using the unique keys – in this case, the beneficiary's PIN code and the provider's biometric. This verification is critical as it creates a confirmation by both parties that the service was rendered. The two-factor authentication process (card plus PIN for beneficiaries and card plus biometric for providers) limits the ability of criminals to fraudulently bill Medicare by posing as a either a provider or beneficiary. It's important to note that this represents two major improvements over the current system: first, a successful transaction requires two parties, and second, each of those parties must provide two-factor authentication of their respective identities.

*(Continued next page)*

## How Medicare CAC works in the doctor's office

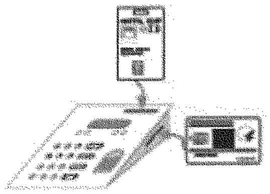


*Provider Credential*

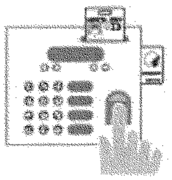


*Beneficiary Credential*

*Both the Medicare Provider and the Beneficiary will be issued Medicare Common Access Card type credentials. The Provider's credential will have a name, photo ID, and a computer chip containing the provider's biographical information, National Provider Identity (NPI) number and their unique biometric key, all securely encrypted. The Beneficiary's card will only have the Beneficiary's name and the secure encrypted computer chip, which contains relevant biographical information, and their Social Security number, which is also their Medicare account number. No longer will a beneficiary's SSN be printed on the front of the card, further protecting the Beneficiary's personal information and privacy.*



*When checking out, both the Beneficiary and the Provider simultaneously insert their cards into the card reader. This ensures that both parties are present to verify and approve the transaction prior to billing CMS.*



*In order to actually process the transaction, the Beneficiary inputs their secret PIN number and the Provider scans their fingerprint biometric, verifying that both parties are who they say they are, and both agree to the transaction.*

**Click here to visit the Secure ID Coalition's website and see a video of the process in action.**

## HOW WILL MEDICARE CAC SOLVE THE PROBLEM?

**Authenticating Identity of Beneficiaries, Providers and Suppliers**

Unauthorized services and product transactions are essentially eliminated since both the secure smart card and the person who owns the key on the card are required to conduct the transaction. This means that phantom billing, fraudulent patient billing and stolen Medicare cards are no longer easy means of bilking Medicare. Furthermore, both parties to the intended transaction must verify the transaction. In addition to imposing strict anti-fraud mechanisms, a Medicare common access card would also reduce processing errors (duplicate or misdirected payments) through electronic verification of data and digitally signed electronic billing processes.

**The Proposed Medicare Common Access Card does not call for use of biometrics for beneficiary authentication.**

As discussed above, the proposal calls for patients to authenticate their identity via the Medicare CAC smart card and a unique PIN. Within the healthcare industry, biometrics are increasingly used for identification due to concerns about patient safety, identity theft, and insurance fraud.

While biometrics are among the most accurate identity verifiers, and are currently used to identify people in many diverse settings including amusement parks, airports, public schools, hospitals, retail outlets and federal government facilities, we are not recommending biometrics for Medicare or Medicaid beneficiaries at this time due to the significant challenges and costs of enrollment.

**Authentication of Medicare Providers and Suppliers**

Biometric authentication is recommended, however, for providers and suppliers in the Medicare CAC system. This would extend to billing agents within a doctor's office or hospital.

Biometrics is the science of identifying people based on certain unique physical characteristics. Examples of types of biometric identification include facial geometry, fingerprint, hand, retina and iris. As part of Medicare CAC, and in a secure smart card environment, biometric data is distilled to a mathematical calculation known as a *template*. Because the template is a representation of the biometric and not the actual image, it cannot be reproduced, copied or stolen. The biometric template is encrypted and securely stored inside the micro-controller embedded in the provider's smart card. At the point of verification, the card is placed in a card reader. No information on that card can be read until the biometric that was provided at enrollment is presented and read. The smart card and the reader would then perform a *one-to-one match* (also known as *match-on-card*) between the template on the card and the live image. The biometric is confirmation that the person to whom the card belongs is present. Because no one would have the associated biometric except for the rightful individual, the system prevents fraudulent behavior. As a result, CMS is afforded the ability to use biometric authentication without maintaining an online national biometric database.

Some biometric systems require an online database to which images are matched when they are presented for verification. This process is called a *one-to-many match*. In the case of Medicare this approach is not recommended because there is no need to try to determine who is filing the claim, only a need to verify that the claim is being filed by the person authorized and to whom the card was issued. The one-to-many match requires constant online access to a central Medicare biometric database and is used to answer the "who is this" question. It would require providers to wait for verification of a one-to-many match process which can take significant time. Having a central Medicare biometric database accessible online is also an invitation for hackers and fraudsters to attempt to breach the system. A one-to-one or match-on-card system answers the "is the person I think it is" question of concern.

For a secure, authenticated Medicare system, a one-to-one match using biometric templates is the recommended approach, giving each provider complete control over their card and verification process. Making authentication easy and less time-consuming benefits both beneficiaries and providers.

**Medicare Beneficiary Privacy and Security**

A secure Medicare smart card strengthens beneficiary privacy and security in a number of ways. First, the beneficiary's Social Security number (SSN), used today as the Medicare Claim Number, will no longer be printed on the card and readily available to identity thieves. The identification information is encrypted and stored safely on the secure embedded chip. Second, information on the card can only be read by an authorized Medicare card-reader, and only when the beneficiary consents to input their correct PIN code. Third, personal information is protected through encryption when transmitted electronically and when stored. The Medicare Common Access Card not only improves the patient's privacy and security in a medical environment, but it strengthens the beneficiary's overall privacy, reducing opportunities for identity theft and fraud.

**Medicare Provider Privacy and Security**

The secure Medicare smart card system similarly protects the privacy and security of the provider's information. NPI's and other personal information will no longer be printed on the front of the card; instead, it will be encoded on the card's secure embedded chip. As with beneficiaries, only an authorized Medicare card reader system can access the information on the card, and then only when the provider has consented to present his biometric. These precautions not only protect the legal card holder's privacy, but also ensure the integrity of the system from fraudsters who steal a provider's card in order to make an unauthorized transaction.

Realizing that providers don't always file the claim to Medicare themselves, the Medicare CAC offers flexibility in that administrative personnel can also be equipped with a Medicare CAC card as an authorized representative of the provider after undergoing the same enrollment process as the provider. To file the claim, the provider's NPI would be securely stored on the authorized representative's smart card. This flexibility alleviates the need for providers to be present to file a claim, and presents no interruption in provider workflow.

**Common Access Card: NIST Approved Open Standards**

In the U.S., open standards for secure identity credentials such as the DOD CAC and PIV cards were developed collaboratively by industry standards organizations with the participation of the U.S. government through the National Institute for Standards and Technology (NIST). The NIST standards were jointly developed to protect both physical and logical (computer networks) government infrastructure against attack.

The Office of Management and Budget, through OMB M-11-11, mandated that every federal agency, including the Department of Defense, utilize secure smart cards to authenticate and verify users for building access and computer access. While it is hard to measure fraud within government agencies, the DOD confirms a 46% reduction in cyber security attacks on the first day of secured logical access implementations in any given department. The U.S. e-Passport is based on the same underlying secure identification technology and was implemented to prevent unauthorized access into the United States.

## WHAT ARE THE BENEFITS OF A MEDICARE SMART CARD TO BENEFICIARIES, PROVIDERS AND TAXPAYERS?

**Benefits to Beneficiaries**
A secure Medicare smart card strengthens beneficiary privacy and security in a number of ways.

- **Social Security Number Removed From Front of Medicare Card**
  The beneficiary's Social Security number (SSN) is no longer printed on the card and readily available to identity thieves. The identification information will be stored safely on the secure embedded chip.
- **Beneficiary Consent**
  Information on the card can only be read by an authorized Medicare card-reader, and only when the beneficiary consents to input their correct PIN code.

- **Personal Information is Encrypted**
  Personal information is protected through encryption when transmitted electronically and when stored.
- **More Funds Available for Legitimate Care**
  Reduction in fraud within the system makes more funds available for legitimate healthcare needs of Medicare beneficiaries.

**Benefits to Providers and Suppliers**
A secure Medicare smart card strengthens providers' privacy and security in a number of ways and enables more efficient business practices.

- **Quicker Processing of Payment**
  Because transactions are verified by both the provider and beneficiary a non-repeatable audit trail is created. This electronic processing eliminates paperwork and streamlines to payment cycle, allowing for quicker and more accurate payment to providers.
- **Billing Accuracy**
  In many cases claims are rejected because of small mistakes or typos. Because the chips verify both the provider and beneficiary all information is electronic, eliminating these types of mistakes.
- **Reduces Need for Recovery Audit Contractors**
  Because both beneficiaries and providers provide proof they are legitimate, payment is pre-approved before it is sent, reducing the need for backend recovery audit contractors.
- **Streamlined Processes Increase Administrative Efficiency**
  Smart cards store basic patient and beneficiary information on the secure chip. That information can be accessed by the provider at point of check-in to identify the correct patient record and eliminate many of the administrative check-in procedures.
- **Protects Medicare Provider Numbers**
  Today provider numbers are widely available and used by thieves billing Medicare for products and services never performed. Using a smart card guarantees that no one can masquerade as the provider and use their number to bill Medicare.
- **Traceability/Audit trail**
  Using a smart card as part of the billing process creates an unrepeatable audit trail definitively verifying the details of each transaction between beneficiary and provider. Since the information is electronically signed and transmitted to CMS processing the information cannot be changed, altered or hacked.

**Benefits to Taxpayers**
While both beneficiaries and providers receive protections and benefits within the system, taxpayers ultimately gain the most significant benefit: reduction of fraud, waste and abuse within the Medicare system. Taxpayer funds can now be targeted directly to those Americans entitled to Medicare benefits, without fear of siphoning by crooks. Such a program will go a

long way towards providing stability and restoring integrity in a program on which so many Americans rely.

## WHERE HAS THIS TYPE OF PROGRAM BEEN SUCCESSFUL?

Smart cards are used in the US and around the world to prevent fraud and reduce costs. Below are just a few examples of smart card deployment that have resulted in significant savings.

**US Healthcare**

While there are myriad examples of smart card implementations in healthcare across the US, we've chosen to highlight two showing cost savings for both large and small hospitals alike.

- Mt. Sinai Hospital, New York City. When Mt. Sinai deployed smart cards to their patients to reduce the number of duplicate or overlaid records in their system, estimated to be close to 15%. The hospital was able to eliminate annual large scale medical record clean-ups which cost the institution $1.8 million and involved over 250,000 duplicate records. Additional benefits included the elimination of the patient clipboard paperwork and reduction in medical errors.

- Memorial Hospital, North Conway, New Hampshire. Memorial Hospital reduced admission errors from 6% of patient records to less than 1% by deploying smart cards, including the reduction of medical record error from a rate of 7% to less than 1%, creating an annual savings of $55,000 for a 35 bed hospital. Patients saw a direct benefit as Memorial Hospital was able to reduce their admission time from 22 minutes to less than 3 minutes – an immediate cost savings of $574,000 in annual employee payroll minutes, which allowed Memorial to redirect staff to other productive tasks.

**International Healthcare**

A number of nations have implemented smart card-based healthcare systems for many reasons beyond fraud reduction, such as security and ensuring administrative cost savings.

- French healthcare system SESAM-Vitale. The French government implemented smart cards in order to verify who was receiving treatment and to quickly provide reimbursements within three to five days as opposed to 3-4 weeks. As a result, the processing cost of a claim within the system was reduced from 1.74 Euros to .27 Euros. With over one billion transactions per year, the transition saves the system over 1.4 billion Euros/year.

- German Ministry of Health. Germany deployed secure smart healthcare cards to approximately 70 million beneficiaries and is currently deploying about 280 thousand health professional cards. The projected achievable program savings in the German national program range from 1.7 to 2.9 billion Euros per year, of which between 800 million to two billion Euros would come from fraud reduction. According to the German Ministry of Health in January 2012, the beneficiary deployment alone has generated annual fraud reduction of 250 million Euros. Provider fraud reduction data will not be available until deployment is completed next year.

- Taiwan. The Taiwanese government implemented one of the longest standing and most comprehensive secure health care cards in the world. Implemented in 2004, the program has issued 24 million patient cards and 300 thousand provider cards. The card data includes not only insurance information but medical information as well. The Bureau of National Health in Taiwan reports that moving from paper to a secure smart card has extended the life of cards by 5-7 years, reduced fraud, saved on administrative costs, and reduced health care spending in general. Taiwan's administrative costs are the lowest in the world at two percent (compared to the U.S. at 31 percent).

**Financial Services**

The smart card technology present in the proposed Medicare CAC Act has been used to great success across the globe to protect identity and secure transactions not only in health care, but in the financial services market as well. Known as "Chip & PIN", the smart card technology has revolutionized the way banks have reduced fraud and identity theft. As testimony to their security and efficacy in fighting fraud, American banks will be introducing Chip & PIN cards to the U.S. market beginning in 2013. Examples of success include:

- United Kingdom Chip & PIN smart card deployment for credit and debit card market. According to a UK Payments Administration reported in 2010, overall fraud losses in the UK fell by 67% and counterfeit card fraud losses have decreased by 77% since 2004, when Chip & PIN was adopted.

- France's Chip & PIN smart card deployment for credit and debit card market. The French banking association GIE CB reported in November 2010 that a fraud ratio of 0.072%, for a total 350 million (USD) – of which $140 million (USD) originated outside France. Five years ago 26% of the system wide fraud was attributed to the Internet and 74% attributed to the real world. Today the numbers are exactly the opposite with 75% attributed to Internet fraud and 25% to real world. GIE CB credits smart cards with reducing real world fraud. For a frame of reference, over 3.5 billion smart card transactions occur every year for a value of $597 billion (USD). There are 58 million smart banking cards in circulation in France (population 64m) with an average of 113 operations/transactions per user.

**A trusted privacy and security tool for the Federal government**

In addition to helping reduce fraud costs around the world, smart cards have been a reliable resource throughout the federal government for identity management and security for more than a decade. Designed on open standards approved by NIST, smart cards use non-proprietary technologies to help secure American's identity and security both home and abroad. Current federal smart card applications include:

- The Department of Defense Common Access Card. Today every federal agency, including the Department of Defense, utilizes secure smart cards to authenticate and verify users for building and computer access. While it is hard to measure fraud within government agencies, the DOD confirms a 46% reduction in cybersecurity attacks on the first day of secured computer access implementation.

- The U.S. Passport. Developed by the State Department and the Government Printing Office, all new passports include a secure smart card computer chip embedded in the back cover. Included to thwart passport counterfeiters, the secure chips protect American citizen's personal information in a manner that prevents tampering and eavesdropping. Since the first year of deployment, 2005, the State Department issued over 75 million ePassports containing the secure smart card chip.

- The Federal Emergency Management Agency's First Responders Authentication Credential (FRAC). In order to ensure local and state emergency response officials are able to collaborate to ensure the public's safety, many identity management challenges must be overcome. The FRAC card meets the task by allowing for interoperability between local, state, and federal first responders. So far, nine states have taken the lead to deploy FRAC credentials for first responders, with many more on the way. It should be noted that all doctors and nurses are considered first responders; as such a Medicare CAC provider card could serve double duty as a FRAC credential, even further reducing implementation costs.

- The American Medical Association/Centers for Disease Control Health Security Card. The American Medical Association's Center for Public Health Preparedness and Disaster Response is working with Center for Disease Control and FEMA to develop a pilot program to show the benefit of a Health Security Card based on smart card technology for patients in the event a disaster or health emergency. Preliminary findings from the pilot excises show 90% of patient using the smart cards rated the care they received as good to excellent, with 75% affirming care as very good or excellent. In December the AMA will issue a final report on the smart card pilot.

## WHAT ARE THE COSTS OF IMPLEMENTING MEDICARE CAC?

Recently, the Smart Card Alliance, an industry non-profit 501 (c)(3) education foundation and trade association, worked with an independent auditor to determine the cost of deploying a smart card based Medicare card system for both providers and beneficiaries *(see attached, DeLeon & Stang Medicare Report)*. The audit was completed in March 2012 with the intent to assist Congress and the Centers for Medicare and Medicaid Services in their efforts to understand the true cost and actual savings of a nation-wide Medicare CAC deployment.

The audit found there are many different elements that must be considered as part of a national Medicare CAC deployment. Because the system will determine real-time eligibility of both providers and beneficiaries, it requires more than just the use of a smart card. Backend infrastructure and readers must be accounted for in any cost estimate. The estimate accounts for 2.6 million providers and 48 million beneficiaries for an overall total of 50.6 million participants.

Because providers will be going through an enrollment process and their biometric information will need to be captured the cost per provider within the system is estimated to be $31.08 per provider. For the beneficiary, the cost is somewhat less, $14.57 per beneficiary, because the beneficiary will receive their smart card via U.S. mail without the requirement of enrollment of biometric capture. The PIN code for the beneficiary could come pre-set as the last four digits of their Social Security number and could easily be changed, if the beneficiary desired upon first use. The total cost for nationwide deployment of Medicare CAC system averages out to $24.24 per participant for a grand total of $1.3 billion for full deployment. These costs are completely inclusive for full deployment and should be evaluated against the return in reductions in fraud, waste and abuse.

## WHAT IS THE RETURN ON INVESTMENT AND WHAT IS IT BASED ON?

The Department of Justice estimates that fraud within the Medicare system costs American taxpayers over $60 billion per year. According to the General Accountability Office (GAO) in 2010 improper payments within Medicare were $48 billion per year. Senator Tom Coburn (R-OK) provided estimates during a March 2, 2011 Senate Finance Committee hearing entitled *Preventing Health Care Fraud: New Tools and Approaches to combat Old Challenges*, fraud and improper payments in the Medicare and Medicaid programs to cost taxpayers between $100 billion - $120 billion per year. Looking at the problem from any prospective, there is a lot of money at stake.

Based on savings reported by the UK, France, Germany and Taiwan across both the healthcare and financial services industries (noted above), it is clear that the use of smart card-based solutions led to a reduction in overall fraud losses upwards of 70%. While the Secure ID Coalition believes that the smart card-based Medicare CAC program will be able to deliver similar results, it is entirely reasonable to assume – at the very least – a cost savings of at least 50%, representing well over $30 billion in eliminated fraud annually at the current rate of fraud. This conservative estimate is further reinforced by the DOD's confirmation of a 46% reduction in cybersecurity attacks on the first day of deployment of the CAC card for computer access.

## RECOMMENDATIONS

- Because the Medicare program is unique, deploying pilot programs or demonstration projects will be an important part of any successful smart card implementation. Five pilot projects in areas where there is a significant amount of fraud will help to identify the specific needs of the Medicare community. These areas could include specific states or regions, similar to metro regions, prioritized by risk categories.

- Planning is a critical part of any pilot program. It is the recommendation of the Secure ID Coalition that the Secretary of HHS be given enough time to plan for the success of the pilots, with a minimum of one year for mapping prior to implementation. Within the mapping period a process by which HHS/CMS establishes metrics to quantify reductions in fraud, waste and abuse must be clearly defined. Further, details of how beneficiary and provider privacy will be protected must be addressed.

- Assuring the interoperability of the new Medicare CAC hardware with existing practice management software systems will also be an important part of the pilot program. Claims are increasingly submitted through electronic interfaces; when including authenticated receipts of rendered services from the new Medicare CAC hardware, claims will be easier to verify by CMS, thus further reducing fraudulent payments and expediting audits. Since the private sector is tasked with the development and implementation of these practice management (PM) systems, the pilot program should be developed to report the essential data needed for determining how best to integrate Medicare CAC hardware into daily medical management practices.

- In order for pilots to provide the requisite amount of data, detailed information about usability, and specific measurable costs and benefits, a minimum duration of eighteen months is recommended for the pilot programs.

- Success of the pilot program will be determined by the established metrics defined prior to the start of the pilot program. Once completed HHS/CMS will be able to verify potential cost savings and benefits and determine the viability of a nationwide deployment without further direction from Congress.

- Once the pilots are completed, HHS/CMS will be able to assess the pilot data and design a nationwide Medicare smart card program that meets the needs of providers, beneficiaries and tax payers.

- Implementing a nationwide program of this scope should be done methodically and over time as to not overload HHS/CMS.

## CONCLUSION

It's everyone's desire to see both the Medicare and Medicaid programs not only survive, but thrive. The cost of waste, fraud and abuse in these systems not only eat away at our tax reserves, but also forces federal and state authorities to spend tens of millions of dollars every year in law enforcement and prosecution costs. It only makes sense to stop the fraud before it happens. In this case, that means implementing a secure smart card to verify and authenticate valid Medicare and Medicaid users at the time of the transaction.

Smart cards are not only a globally recognized tool to help eliminate medical and financial fraud, but a trusted tool of the federal government in assuring identity across a number of critical applications. If Congress were to implement a smart card technology solution – such as described in the Medicare Common Access Card Act – it would have the potential to save American taxpayers over half of the estimated $60 billion per year cost of fraud. With over 48 million seniors, that comes out to approximately $1,250 of fraud per recipient per year. However, for a one-time investment of less than $25 per beneficiary, the federal government will realize a cost savings of over $612.50 per beneficiary per year – a return on investment 24 times over.

Everyone in Congress wants to preserve Medicare for the next generation of beneficiaries; Medicare CAC does this without having to raise taxes, eliminate benefits, or cut reimbursements. In our opinion, this is the best outcome of all possible solutions.

Mr. Chairman, Ranking Member, and Members of the Committee: the Secure ID Coalition stands ready to assist Congress in helping save the Medicare and Medicaid programs. We look forward to working with you and answering any questions you may have.

## QUESTIONS & ANSWERS

**If the beneficiary does not have their card, will they be denied access to care?**
Absolutely not. CMS will need to establish a policy for how to process claims that are outside of the validated and authenticated Medicare CAC system.

Some cards will get lost, whether it's because of illness or just plain forgetfulness; it happens today in every program. This is not a technology issue, but a question of policy on how CMS would treat billings that have not been authenticated. In the case of beneficiaries who need to have a caretaker or legal guardian tend to their medical needs because they cannot communicate, a special caretaker credential could be issued to them.

**How will personal privacy be protected using a smart card?**
Both privacy and security must be considered fundamental design goals for any personal ID system and must be factored into the specification of the ID system's policies, processes, architectures, and technologies. The use of smart cards strengthens the ability of the system to protect individual privacy and secure personal information.

Unlike other identification technologies, smart cards can provide authenticated and authorized information access, implementing a personal firewall for the individual and releasing only the information required when the card is presented. Smart card technology provides strong privacy-enabling features for ID system designers, including the ability to:

- Support anonymous and pseudonymous schemes
- Segregate multiple applications on the card
- Support multiple single-purpose IDs
- Provide authentication of other system components
- Provide on-card matching of cardholder verification information
- Implement strong security for both the ID card and personal data

Smart cards trust nothing until proven otherwise. For example, smart cards can require cardholders to authenticate themselves first (with a PIN or biometric) before the cards will release any data. And smart cards support encryption, providing patient data privacy and enabling at-home or self-service applications in suspect or untrusted environments to be secure.

The smart card's embedded secure microcontroller provides it with built-in tamper resistance and the unique ability to securely store large amounts of data, carry out own on-card functions (e.g., encryption and digital signatures), and interact intelligently with a smart card reader.

**In case a beneficiary card is lost, how secure is one's personal information?**
If the card is lost, the data on the card is secure and not readable without the individual's PIN code. Further, all information stored in the card cannot be read unless accessed via an authorized, authenticated reader. An attempt to hack the chip on the card would destroy the information in the process, because the chips are designed to shut down under brute force

attacks. Once the card is reported lost or stolen the system will no longer recognize it and it becomes completely useless. One of the significant benefits that will reduce medical ID theft is that the card will no longer have the beneficiary's social security number printed on it.

**In the case of beneficiaries seeking care outside their home region, how will the cards work?**
This is an issue that exists today with paper Medicare cards containing SSNs in full view. The secure Medicare smart cards will work in any authenticated provider reader and benefits will be fully available nation-wide under existing Medicare services guidelines. During the pilot program, CMS would treat beneficiaries seeking care outside their home region under the same polices as if the beneficiary had lost their card.

**Would a smart card program work with other program integrity efforts CMS has already deployed?**
A smart card program will complement existing programs initially and, over time, the SIDC anticipates CMS would do away with some of the reactive initiatives underway due to the success of the smart card program to reduce fraud, waste and abuse in the system. Unlike the programs currently underway that search for fraud after the transaction has been process and the money disbursed, the smart card program is a proactive fraud prevention approach. To date, no proactive initiatives have been put forth by CMS.

## APPENDIX

### ADDITIONAL RESOURCES

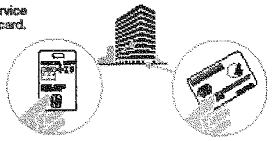
- Smart Cards and Biometrics in Healthcare Identity Applications, Smart Card Alliance Healthcare Council white paper, May 2012
- Benefits of Smart Cards versus Magnetic Stripe Cards for Healthcare Applications, Smart Card Alliance Healthcare Council brief, December 2011
- Effective Healthcare Identity Management: A Necessary First Step for Improving U.S. Healthcare Information Systems – A Smart Card Alliance Brief for Government Policy Makers and Other Stakeholders, Smart Card Alliance Healthcare Council and Identity Council brief, March 2009

### ATTACHED DOCUMENTS

- Secure ID Coalition, *Medicare Common Access Card: How Does It Work*, 2012.
- DeLeon & Stang Certified Public Accountants and Advisors, *Smart Card Alliance Projected Schedule of Costs To Deploy Secure ID Card and Related Fraud Reduction Cost Savings and Return on Investment with Independent Accounts' Report,* June 27, 2012.
- *AARP Joins Bipartisan Effort to Prevent Identity Theft of Medicare Beneficiaries*, September 14, 2011.
- Lawrence Carbonaro, *Converting to LifeMed*, Memorial Hospital of Conway, New Hampshire, 2012. (Memorial Hospital report on savings realized from conversion to LifeMed, a smart card-based health information system.)
- Theresa Min-Hyung Lee, *Comparative Study of Taiwanese Health Care System, in* The Ampersand Journal, Issue IV 42 (McGill University), 2011.

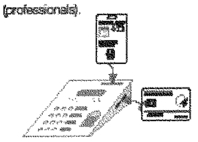
## How it works
# Medicare Common Access Card

1 Medicare beneficiaries and service providers receive a secure ID card.

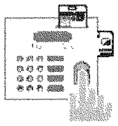


The smart card contains a computer chip that fights fraud and protects privacy.

What's stored on the ID card:
- A unique Medicare identity.
- A digital picture of the healthcare professional.
- A PIN code (beneficiaries) or biometric (professionals).
- Match-on-card software:
  PIN or biometric stays in the card.



2 At the doctor's office, both the ID cards are inserted into the reader. The chip on the card electronically confirms the card is legitimate.

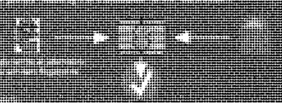


3 The doctor confirms his or her identity by touching the biometric reader, and the beneficiary by entering a PIN code, proving both were there.

4 Transaction is confirmed and a secure authenticated information packet is sent to the payment processor.

[illegible]

[illegible]



[illegible]

[illegible]

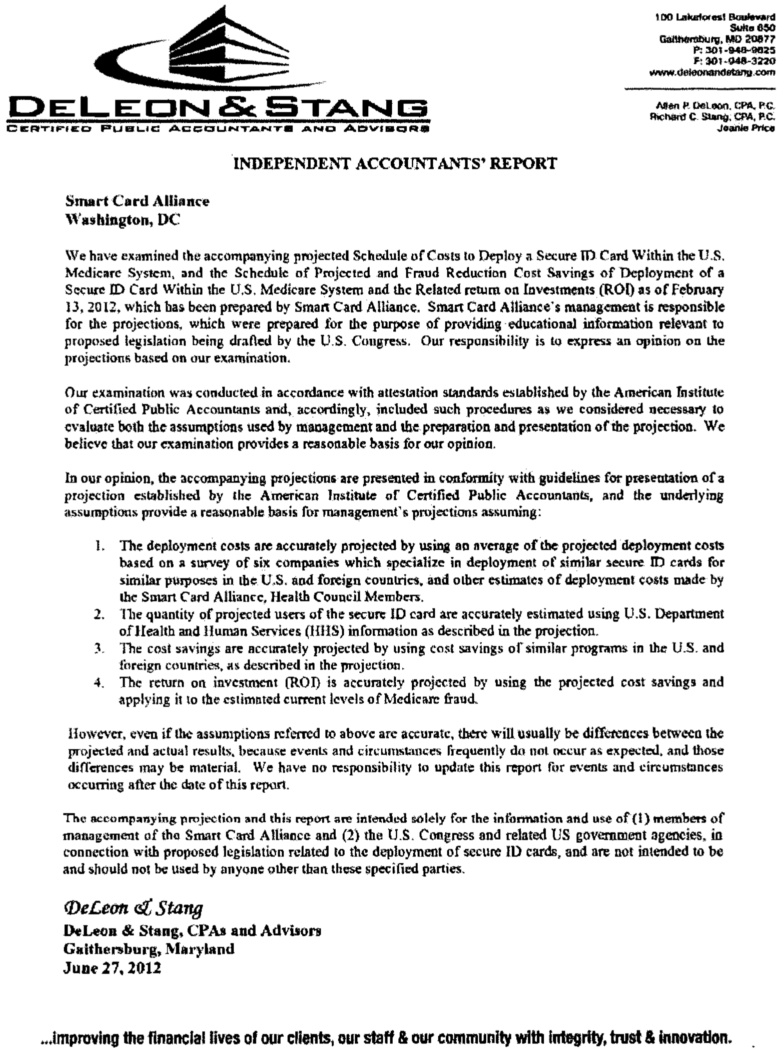
[illegible]

Medicare Common Access Cards [illegible] Medicare Fraud

*For more information contact the Secure ID Coalition | www.secureidcoalition.org | p:202-464-4000*

**SMART CARD ALLIANCE**
**PROJECTED SCHEDULE OF COSTS**
**TO DEPLOY SECURE ID CARD**
**AND RELATED FRAUD REDUCTION COST**
**SAVINGS AND RETURN ON INVESTMENT**
**WITH**
**INDEPENDENT ACCOUNTANTS' REPORT**

DELEON & STANG



DELEON & STANG
CERTIFIED PUBLIC ACCOUNTANTS AND ADVISORS

100 Lakeforest Boulevard
Suite 650
Gaithersburg, MD 20877
P: 301-948-9825
F: 301-948-3220
www.deleonandstang.com

Allen P. DeLeon, CPA, P.C.
Richard C. Stang, CPA, P.C.
Joanie Price

## INDEPENDENT ACCOUNTANTS' REPORT

**Smart Card Alliance**
**Washington, DC**

We have examined the accompanying projected Schedule of Costs to Deploy a Secure ID Card Within the U.S. Medicare System, and the Schedule of Projected and Fraud Reduction Cost Savings of Deployment of a Secure ID Card Within the U.S. Medicare System and the Related return on Investments (ROI) as of February 13, 2012, which has been prepared by Smart Card Alliance. Smart Card Alliance's management is responsible for the projections, which were prepared for the purpose of providing educational information relevant to proposed legislation being drafted by the U.S. Congress. Our responsibility is to express an opinion on the projections based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included such procedures as we considered necessary to evaluate both the assumptions used by management and the preparation and presentation of the projection. We believe that our examination provides a reasonable basis for our opinion.

In our opinion, the accompanying projections are presented in conformity with guidelines for presentation of a projection established by the American Institute of Certified Public Accountants, and the underlying assumptions provide a reasonable basis for management's projections assuming:

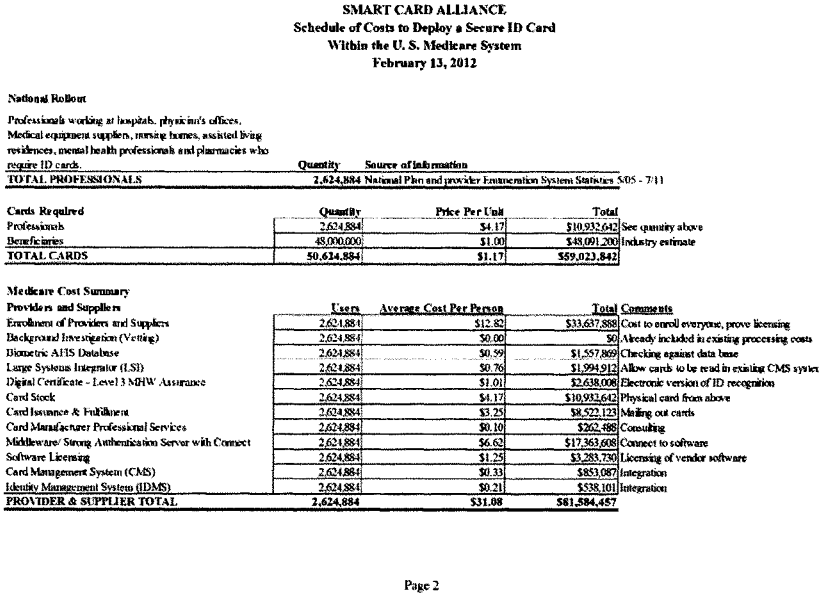
1. The deployment costs are accurately projected by using an average of the projected deployment costs based on a survey of six companies which specialize in deployment of similar secure ID cards for similar purposes in the U.S. and foreign countries, and other estimates of deployment costs made by the Smart Card Alliance, Health Council Members.
2. The quantity of projected users of the secure ID card are accurately estimated using U.S. Department of Health and Human Services (HHS) information as described in the projection.
3. The cost savings are accurately projected by using cost savings of similar programs in the U.S. and foreign countries, as described in the projection.
4. The return on investment (ROI) is accurately projected by using the projected cost savings and applying it to the estimated current levels of Medicare fraud.

However, even if the assumptions referred to above are accurate, there will usually be differences between the projected and actual results, because events and circumstances frequently do not occur as expected, and those differences may be material. We have no responsibility to update this report for events and circumstances occurring after the date of this report.

The accompanying projection and this report are intended solely for the information and use of (1) members of management of the Smart Card Alliance and (2) the U.S. Congress and related US government agencies, in connection with proposed legislation related to the deployment of secure ID cards, and are not intended to be and should not be used by anyone other than these specified parties.

*DeLeon & Stang*
**DeLeon & Stang, CPAs and Advisors**
**Gaithersburg, Maryland**
**June 27, 2012**

**...improving the financial lives of our clients, our staff & our community with integrity, trust & innovation.**



SMART CARD ALLIANCE
Schedule of Costs to Deploy a Secure ID Card
Within the U. S. Medicare System
February 13, 2012

National Rollout

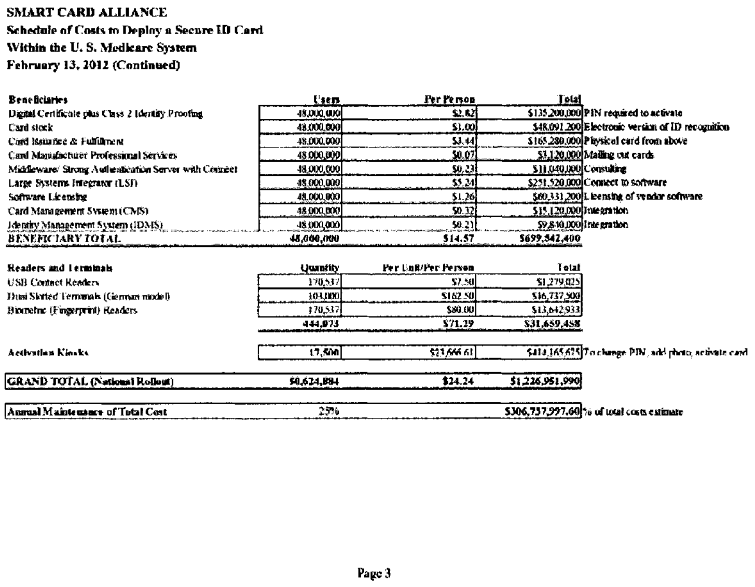
| Professionals working at hospitals, physician's offices, Medical equipment suppliers, nursing homes, assisted living residences, mental health professionals and pharmacies who require ID cards. | Quantity | Source of information |
|---|---|---|
| **TOTAL PROFESSIONALS** | **2,624,884** | National Plan and provider Enumeration System Statistics 5/05 - 7/11 |

| Cards Required | Quantity | Price Per Unit | Total | |
|---|---|---|---|---|
| Professionals | 2,624,884 | $4.17 | $10,932,642 | See quantity above |
| Beneficiaries | 48,000,000 | $1.00 | $48,091,200 | Industry estimate |
| **TOTAL CARDS** | **50,624,884** | **$1.17** | **$59,023,842** | |

Medicare Cost Summary

| Providers and Suppliers | Users | Average Cost Per Person | Total | Comments |
|---|---|---|---|---|
| Enrollment of Providers and Suppliers | 2,624,884 | $12.82 | $33,637,888 | Cost to enroll everyone, prove licensing |
| Background Investigation (Vetting) | 2,624,884 | $0.00 | $0 | Already included in existing processing costs |
| Biometric AFIS Database | 2,624,884 | $0.59 | $1,557,869 | Checking against data base |
| Large Systems Integrator (LSI) | 2,624,884 | $0.76 | $1,994,912 | Allow cards to be read in existing CMS syster |
| Digital Certificate - Level 3 MHW Assurance | 2,624,884 | $1.01 | $2,638,008 | Electronic version of ID recognition |
| Card Stock | 2,624,884 | $4.17 | $10,932,642 | Physical card from above |
| Card Issuance & Fulfillment | 2,624,884 | $3.25 | $8,522,123 | Mailing out cards |
| Card Manufacturer Professional Services | 2,624,884 | $0.10 | $262,488 | Consulting |
| Middleware/ Strong Authentication Server with Connect | 2,621,884 | $6.62 | $17,363,608 | Connect to software |
| Software Licensing | 2,624,884 | $1.25 | $3,283,730 | Licensing of vendor software |
| Card Management System (CMS) | 2,624,884 | $0.33 | $853,087 | Integration |
| Identity Management System (IDMS) | 2,624,884 | $0.21 | $538,101 | Integration |
| **PROVIDER & SUPPLIER TOTAL** | **2,624,884** | **$31.08** | **$81,584,457** | |

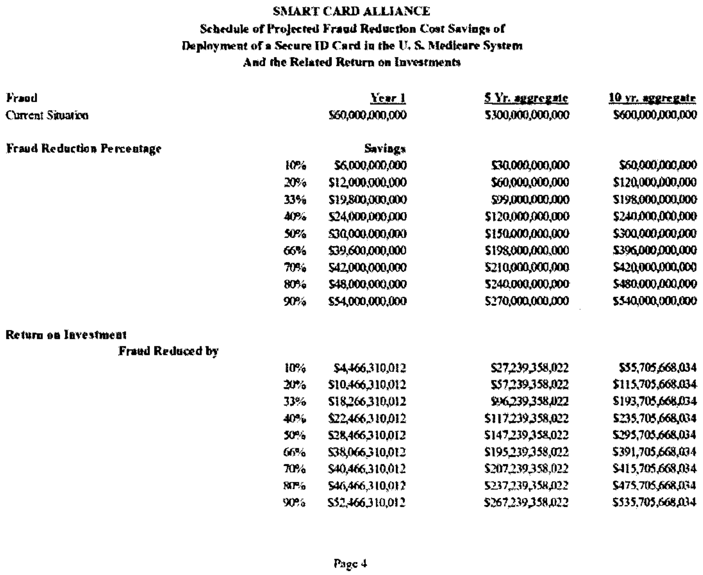
Page 2



**SMART CARD ALLIANCE**
**Schedule of Costs to Deploy a Secure ID Card**
**Within the U. S. Medicare System**
**February 13, 2012 (Continued)**

| **Beneficiaries** | **Users** | **Per Person** | **Total** | |
|---|---|---|---|---|
| Digital Certificate plus Class 2 Identity Proofing | 48,000,000 | $2.82 | $135,200,000 | PIN required to activate |
| Card stock | 48,000,000 | $1.00 | $48,091,200 | Electronic version of ID recognition |
| Card Issuance & Fulfillment | 48,000,000 | $3.44 | $165,280,000 | Physical card from above |
| Card Manufacturer Professional Services | 48,000,000 | $0.07 | $3,120,000 | Mailing out cards |
| Middleware/ Strong Authentication Server with Connect | 48,000,000 | $0.23 | $11,040,000 | Consulting |
| Large Systems Integrator (LSI) | 48,000,000 | $5.24 | $251,520,000 | Connect to software |
| Software Licensing | 48,000,000 | $1.26 | $60,331,200 | Licensing of vendor software |
| Card Management System (CMS) | 48,000,000 | $0.32 | $15,120,000 | Integration |
| Identity Management System (IDMS) | 48,000,000 | $0.21 | $9,840,000 | Integration |
| **BENEFICIARY TOTAL** | **48,000,000** | **$14.57** | **$699,542,400** | |
| | | | | |
| **Readers and Terminals** | **Quantity** | **Per Unit/Per Person** | **Total** | |
| USB Contact Readers | 170,537 | $7.50 | $1,279,025 | |
| Dual Slotted Terminals (German model) | 103,000 | $162.50 | $16,737,500 | |
| Biometric (Fingerprint) Readers | 170,537 | $80.00 | $13,642,933 | |
| | **444,073** | **$71.29** | **$31,659,458** | |
| | | | | |
| **Activation Kiosks** | 17,500 | $23,666.61 | $414,165,675 | To change PIN, add photo, activate card |
| | | | | |
| **GRAND TOTAL (National Rollout)** | **50,624,894** | **$24.24** | **$1,226,951,990** | |
| | | | | |
| **Annual Maintenance of Total Cost** | 25% | | **$306,737,997.60** | % of total costs estimate |

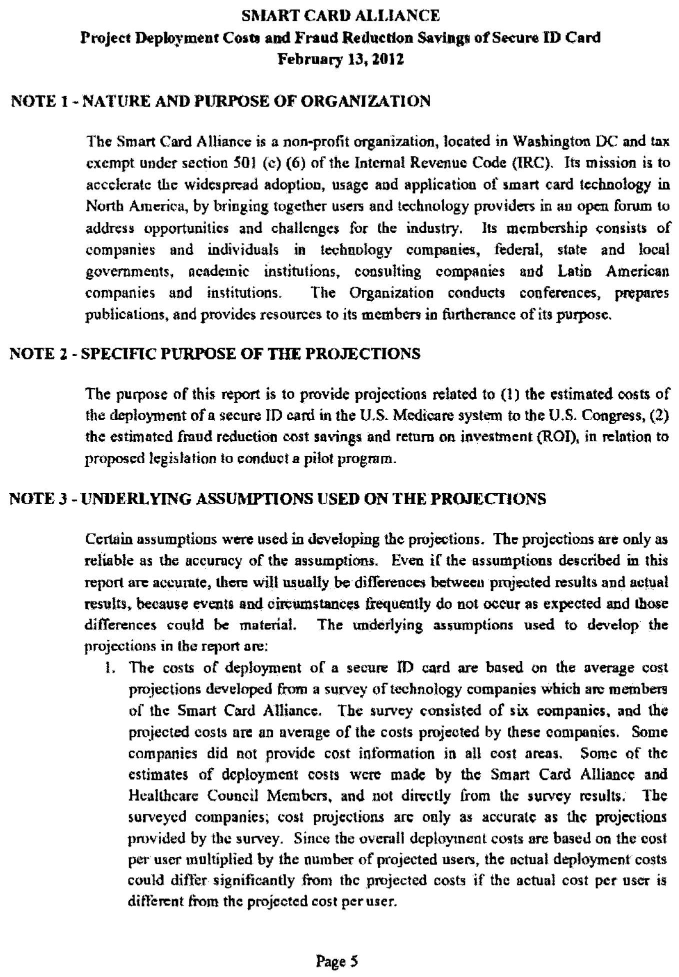
Page 3



**SMART CARD ALLIANCE**
**Schedule of Projected Fraud Reduction Cost Savings of**
**Deployment of a Secure ID Card in the U. S. Medicare System**
**And the Related Return on Investments**

| **Fraud** | | <u>**Year 1**</u> | <u>**5 Yr. aggregate**</u> | <u>**10 yr. aggregate**</u> |
|---|---|---|---|---|
| Current Situation | | $60,000,000,000 | $300,000,000,000 | $600,000,000,000 |
| | | | | |
| **Fraud Reduction Percentage** | | **Savings** | | |
| | 10% | $6,000,000,000 | $30,000,000,000 | $60,000,000,000 |
| | 20% | $12,000,000,000 | $60,000,000,000 | $120,000,000,000 |
| | 33% | $19,800,000,000 | $99,000,000,000 | $198,000,000,000 |
| | 40% | $24,000,000,000 | $120,000,000,000 | $240,000,000,000 |
| | 50% | $30,000,000,000 | $150,000,000,000 | $300,000,000,000 |
| | 66% | $39,600,000,000 | $198,000,000,000 | $396,000,000,000 |
| | 70% | $42,000,000,000 | $210,000,000,000 | $420,000,000,000 |
| | 80% | $48,000,000,000 | $240,000,000,000 | $480,000,000,000 |
| | 90% | $54,000,000,000 | $270,000,000,000 | $540,000,000,000 |
| | | | | |
| **Return on Investment** | | | | |
| **Fraud Reduced by** | | | | |
| | 10% | $4,466,310,012 | $27,239,358,022 | $55,705,668,034 |
| | 20% | $10,466,310,012 | $57,239,358,022 | $115,705,668,034 |
| | 33% | $18,266,310,012 | $96,239,358,022 | $193,705,668,034 |
| | 40% | $22,466,310,012 | $117,239,358,022 | $235,705,668,034 |
| | 50% | $28,466,310,012 | $147,239,358,022 | $295,705,668,034 |
| | 66% | $38,066,310,012 | $195,239,358,022 | $391,705,668,034 |
| | 70% | $40,466,310,012 | $207,239,358,022 | $415,705,668,034 |
| | 80% | $46,466,310,012 | $237,239,358,022 | $475,705,668,034 |
| | 90% | $52,466,310,012 | $267,239,358,022 | $535,705,668,034 |

Page 4



**SMART CARD ALLIANCE**
**Project Deployment Costs and Fraud Reduction Savings of Secure ID Card**
**February 13, 2012**

**NOTE 1 - NATURE AND PURPOSE OF ORGANIZATION**

The Smart Card Alliance is a non-profit organization, located in Washington DC and tax exempt under section 501 (c) (6) of the Internal Revenue Code (IRC). Its mission is to accelerate the widespread adoption, usage and application of smart card technology in North America, by bringing together users and technology providers in an open forum to address opportunities and challenges for the industry. Its membership consists of companies and individuals in technology companies, federal, state and local governments, academic institutions, consulting companies and Latin American companies and institutions. The Organization conducts conferences, prepares publications, and provides resources to its members in furtherance of its purpose.

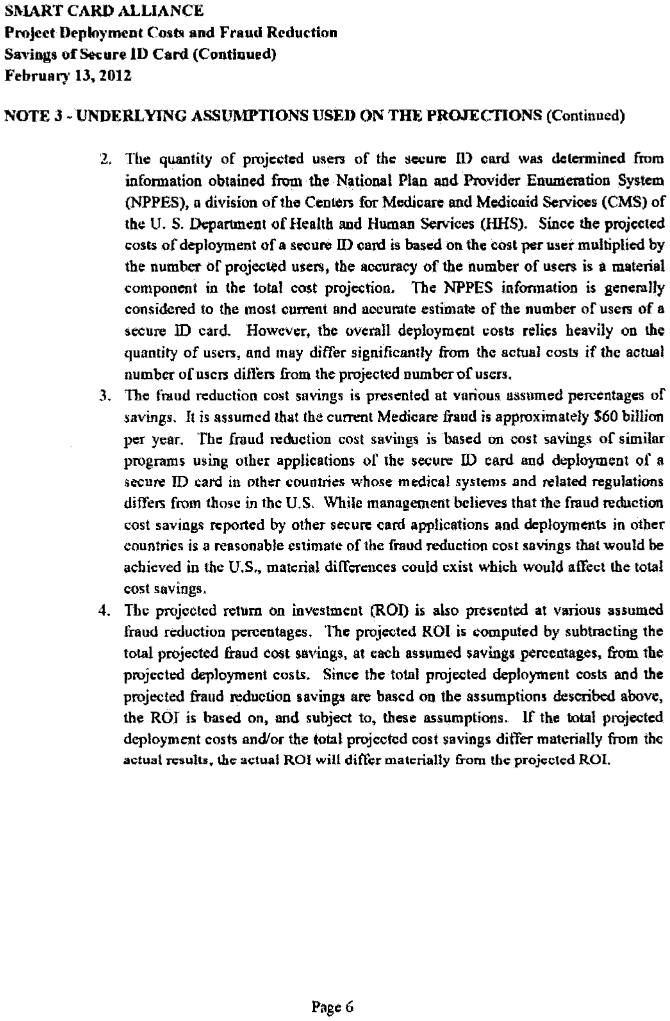
**NOTE 2 - SPECIFIC PURPOSE OF THE PROJECTIONS**

The purpose of this report is to provide projections related to (1) the estimated costs of the deployment of a secure ID card in the U.S. Medicare system to the U.S. Congress, (2) the estimated fraud reduction cost savings and return on investment (ROI), in relation to proposed legislation to conduct a pilot program.

**NOTE 3 - UNDERLYING ASSUMPTIONS USED ON THE PROJECTIONS**

Certain assumptions were used in developing the projections. The projections are only as reliable as the accuracy of the assumptions. Even if the assumptions described in this report are accurate, there will usually be differences between projected results and actual results, because events and circumstances frequently do not occur as expected and those differences could be material. The underlying assumptions used to develop the projections in the report are:

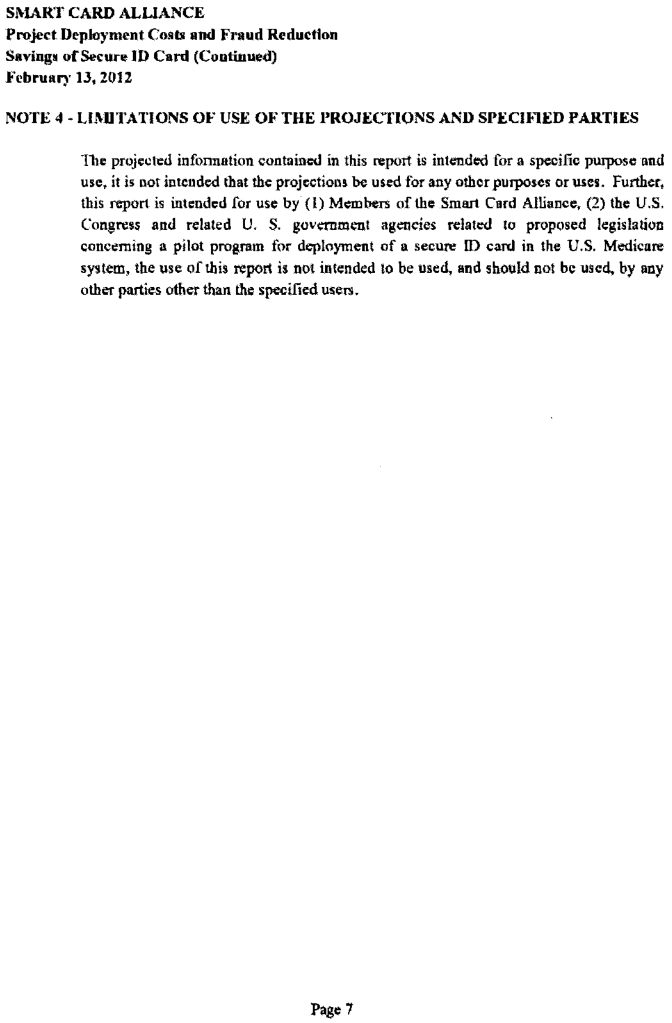
1. The costs of deployment of a secure ID card are based on the average cost projections developed from a survey of technology companies which are members of the Smart Card Alliance. The survey consisted of six companies, and the projected costs are an average of the costs projected by these companies. Some companies did not provide cost information in all cost areas. Some of the estimates of deployment costs were made by the Smart Card Alliance and Healthcare Council Members, and not directly from the survey results. The surveyed companies; cost projections are only as accurate as the projections provided by the survey. Since the overall deployment costs are based on the cost per user multiplied by the number of projected users, the actual deployment costs could differ significantly from the projected costs if the actual cost per user is different from the projected cost per user.



**SMART CARD ALLIANCE**
**Project Deployment Costs and Fraud Reduction**
**Savings of Secure ID Card (Continued)**
**February 13, 2012**

**NOTE 3 - UNDERLYING ASSUMPTIONS USED ON THE PROJECTIONS** (Continued)

2. The quantity of projected users of the secure ID card was determined from information obtained from the National Plan and Provider Enumeration System (NPPES), a division of the Centers for Medicare and Medicaid Services (CMS) of the U. S. Department of Health and Human Services (HHS). Since the projected costs of deployment of a secure ID card is based on the cost per user multiplied by the number of projected users, the accuracy of the number of users is a material component in the total cost projection. The NPPES information is generally considered to the most current and accurate estimate of the number of users of a secure ID card. However, the overall deployment costs relies heavily on the quantity of users, and may differ significantly from the actual costs if the actual number of users differs from the projected number of users.
3. The fraud reduction cost savings is presented at various assumed percentages of savings. It is assumed that the current Medicare fraud is approximately $60 billion per year. The fraud reduction cost savings is based on cost savings of similar programs using other applications of the secure ID card and deployment of a secure ID card in other countries whose medical systems and related regulations differs from those in the U.S. While management believes that the fraud reduction cost savings reported by other secure card applications and deployments in other countries is a reasonable estimate of the fraud reduction cost savings that would be achieved in the U.S., material differences could exist which would affect the total cost savings.
4. The projected return on investment (ROI) is also presented at various assumed fraud reduction percentages. The projected ROI is computed by subtracting the total projected fraud cost savings, at each assumed savings percentages, from the projected deployment costs. Since the total projected deployment costs and the projected fraud reduction savings are based on the assumptions described above, the ROI is based on, and subject to, these assumptions. If the total projected deployment costs and/or the total projected cost savings differ materially from the actual results, the actual ROI will differ materially from the projected ROI.



**SMART CARD ALLIANCE**
**Project Deployment Costs and Fraud Reduction**
**Savings of Secure ID Card (Continued)**
**February 13, 2012**

**NOTE 4 - LIMITATIONS OF USE OF THE PROJECTIONS AND SPECIFIED PARTIES**

The projected information contained in this report is intended for a specific purpose and use, it is not intended that the projections be used for any other purposes or uses. Further, this report is intended for use by (1) Members of the Smart Card Alliance, (2) the U.S. Congress and related U. S. government agencies related to proposed legislation concerning a pilot program for deployment of a secure ID card in the U.S. Medicare system, the use of this report is not intended to be used, and should not be used, by any other parties other than the specified users.

# AARP Joins Bipartisan Effort to Prevent Identity Theft of Medicare Beneficiaries

## AARP today endorsed the Medicare Common Access Card Act of 2011

From: Press Center | September 14, 2011

FOR IMMEDIATE RELEASE
September 14, 2011

CONTACT:
AARP Media Relations, 202-434-2560

AARP Joins Bipartisan Effort to Prevent Identity Theft of Medicare Beneficiaries

WASHINGTON – AARP today endorsed the Medicare Common Access Card Act of 2011 in a letter to U.S. Senators Mark Kirk and Ron Wyden as well as U.S. Representatives Jim Gerlach and Earl Blumenauer. The bill will create a secure Medicare identification card pilot program for beneficiaries located in five geographic areas nationwide. This bipartisan and bicameral piece of legislation introduced today will replace paper Medicare cards with secure cards that carry the personal information electronically of individuals in the program.

Excerpts of the letter of support from Joyce A. Rogers, AARP Senior Vice President, are below:

"On behalf of AARP's millions of members, we are pleased to endorse the Medicare Common Access Card Act of 2011. Your legislation will create a secure card pilot program under the Medicare program.

"Older Americans are particularly vulnerable to the dangers of identity theft. Your legislation will pilot a program to replace the current paper Medicare card with a smart card that would store the beneficiary's personal information electronically on a computer chip, and would require both beneficiaries and providers to confirm receipt of services at the time services were provided. Similar technology currently exists for Department of Defense personnel.

"Your legislation not only provides enhanced information security, but will also help to reduce fraud in the Medicare program by verifying the identity of both Medicare beneficiaries and providers. Medicare dollars should be spent on necessary services and not lost to fraudulent activities."

For a copy of the full-text of the letter, please contact AARP Media Relations by phone at (202) 434-2560 or via email at media@aarp.org.

About AARP:
AARP is a nonprofit, nonpartisan organization with a membership that helps people 50+ have independence, choice and control in ways that are beneficial and affordable to them and society as a whole. AARP does not endorse candidates for public office or make contributions to either political campaigns or candidates. We produce AARP The Magazine, the definitive voice for 50+ Americans and the world's largest-circulation magazine with nearly 35 million readers; AARP Bulletin, the go-to news source for AARP's millions of members and Americans 50+; AARP VIVA, the only bilingual U.S. publication dedicated exclusively to the 50+ Hispanic community; and our website, AARP.org. AARP Foundation is an affiliated charity that provides security, protection, and empowerment to older persons in need with support from thousands of volunteers, donors, and sponsors. We have staffed offices in all 50 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands.

http://www.aarp.org/about-aarp/press-center/info-09-2011/aarp-joins-bipartisan-effort-to-prevent-identity-theft-of-medicare-beneficiaries.print.html

Memorial
Hospital

## Converting to LifeMed

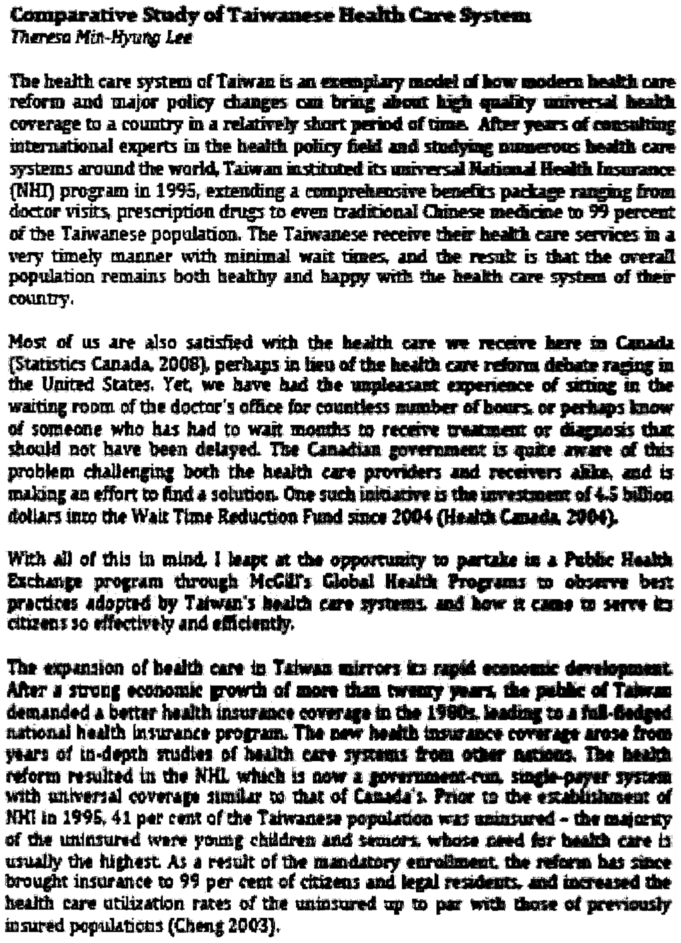
By: Lawrence Carbonaro
Director, Purchasing, Patient Access & HIS

The Memorial Hospital, North Conway, NH **(35 beds, 100,000 annual patient visits and over $300,000 in administrative savings annually, not including the marketing advantages)**

- □ **Decreased admissions error rate from 6% to less than 1%** *We average 1500 registrations a week, thus 90 records that used to require manual intervention to fix before billing; with LifeMed we no longer require that effort.)*
- □ **Elimination of clip board and paper** *(We went paperless as a result of LifeMed. We used to print a cover sheet to give to the patient with each registration, this is no longer required. 156 cases of paper plus toner are no longer used, no shredding or storage.)*
- □ **Reduced duplicate records from 7% to less than 1%** *(an annual cost savings of **$35K-$55k** for scrubbing records. No numbers reported for medical errors due to incorrect chart)*
- □ **Reduced admission time from 22 minutes to less than 3 minutes** *(average salary equaling $18.13 an hour and a average saving of 19 minutes equals a soft cost saving of $5.74 per patient times 100,000 patents annually. Registration saving of **$574,000** of annual employee payroll minutes allowing Memorial to redirect staff to other productive tasks, like accurate insurance billings, etc. - LifeMed soft projection).* See reduced staff below
- □ **Reduced medical record error from 7% to less than 1%** *(unreported cost savings but includes billing losses, medical procedure losses, medical errors, lawsuits, etc)*
- □ **Reduced PAC System errors to less than 1%** *(Hard to quantify but PACs errors were occurring about 150 annually, now they are rare. Pacs administrator time was 3+ hours to fix each error. About **$25K** savings, assumed pay would be greater than $100K)*
- □ **Reduced full time staff requirements from 21 to 15** *(Annual savings equates to **$224,640** using a burdened salary of $37,440 annually).*
- □ **Decreased insurance A/R from 55+ to 42 days** *(unreported saving; Current days are still reducing in A/R and is now below 41 days).*
- □ **Increased Press-Ganey patient satisfaction by 10% within first 60 days** *(Memorial's now in the top 5% of all hospitals with satisfaction in registration - this was a major issue as our patient dissatisfaction began at admission even before the patient saw an employee or clinician. Patient satisfaction influenced patient and employee retention and employee gratification).*

Areas of Savings not reported or financially measured as of the date of these Administrative Measures:

- □ Patient Satisfaction Increase
- □ Diminished Registration Errors
- □ Diminished in Duplicate Records
- □ Diminished in Record Errors
- □ Elimination of Registration Paper
- □ Decreased Insurance A/R



## Comparative Study of Taiwanese Health Care System

*Theresa Min-Hyung Lee*

The health care system of Taiwan is an exemplary model of how modern health care reform and major policy changes can bring about high quality universal health coverage to a country in a relatively short period of time. After years of consulting international experts in the health policy field and studying numerous health care systems around the world, Taiwan instituted its universal National Health Insurance (NHI) program in 1995, extending a comprehensive benefits package ranging from doctor visits, prescription drugs to even traditional Chinese medicine to 99 percent of the Taiwanese population. The Taiwanese receive their health care services in a very timely manner with minimal wait times, and the result is that the overall population remains both healthy and happy with the health care system of their country.

Most of us are also satisfied with the health care we receive here in Canada (Statistics Canada, 2008), perhaps in lieu of the health care reform debate raging in the United States. Yet, we have had the unpleasant experience of sitting in the waiting room of the doctor's office for countless number of hours, or perhaps know of someone who has had to wait months to receive treatment or diagnosis that should not have been delayed. The Canadian government is quite aware of this problem challenging both the health care providers and receivers alike, and is making an effort to find a solution. One such initiative is the investment of 4.5 billion dollars into the Wait Time Reduction Fund since 2004 (Health Canada, 2004).

With all of this in mind, I leapt at the opportunity to partake in a Public Health Exchange program through McGill's Global Health Programs to observe best practices adopted by Taiwan's health care systems, and how it came to serve its citizens so effectively and efficiently.

The expansion of health care in Taiwan mirrors its rapid economic development. After a strong economic growth of more than twenty years, the public of Taiwan demanded a better health insurance coverage in the 1980s, leading to a full-fledged national health insurance program. The new health insurance coverage arose from years of in-depth studies of health care systems from other nations. The health reform resulted in the NHI, which is now a government-run, single-payer system with universal coverage similar to that of Canada's. Prior to the establishment of NHI in 1995, 41 per cent of the Taiwanese population was uninsured – the majority of the uninsured were young children and seniors, whose need for health care is usually the highest. As a result of the mandatory enrollment, the reform has since brought insurance to 99 per cent of citizens and legal residents, and increased the health care utilization rates of the uninsured up to par with those of previously insured populations (Cheng 2003).

Despite several similarities with the Canadian health care system as a whole, there are some notable differences between the two systems. Firstly, Taiwan's health care coverage is more comprehensive. It covers services that Canadians are usually pay out-of-pocket, or through supplemental health insurance. These services include prescription drugs, dental care, vision care and traditional Chinese medicine (Cheng 2003).

Secondly, patients are free to see doctors of any specialty without going through a referral or 'gatekeeper' system. There are also no limitations on the type of hospital that from which the patients can receive their health care. Due to the absence of a gatekeeper system, there is no need to first see your primary healthcare provider to receive a referral to see a specialist. As a result, there is virtually no waiting list for a visit to the doctor's office. There is also freedom to choose between health care facilities, ranging from small public health clinics to large private hospitals that offer comfort with luxurious décor.

Upon observing and learning about many health care facilities (including public and private clinics, large teaching hospitals, major public hospitals and private hospitals alike, to a psychiatric hospital, a Traditional Chinese Medical hospital and a regional Centre for Disease Control), and discussing with and listening to doctors, nurses, professors and medical students, the facilities appeared to be spectacular, well-equipped with modern technology; and the breadth of services available to the Taiwanese population presented was truly impressive.

With high health indicators comparable to any developed nation – infant mortality rate of 5.26 per 1000 births; and life expectancy at birth of 75.34 years for men and 81.2 years for women (Central Intelligence Agency, 2010) – it was clear that Taiwan was providing health care that successfully sustains a healthy general population. Furthermore, a closer look at Taiwan's national health expenditure rates indicate that this was being achieved at a fraction of the cost of other nations: only 6 percent of Taiwan's GDP is spent on healthcare, compared to 10 percent for Canada and 16 percent for the United States (Organization for Economic Cooperation and Development, 2010). Since its implementation, NHI has had a public satisfaction rating ranging from 70 to 80 per cent, dipping low only in the years where new policies introduced higher insurance rates (Cheng 2003). It remained unclear how Taiwan managed to sustain a health care system achieving similar, if not better, results than that of Canada's and the United States'

The NHI is publicly funded and financed on income-based premiums as opposed to general tax revenues. The premiums are based on payroll taxes paid by the employer, the employee and the government in varying amounts depending on different population groups. Most people who are employed pay 30 per cent of the premium, while their employee pays 60 per cent and the government subsidizes the remaining 10 per cent. The self-employed pay 100 per cent of the premium, and individuals from a low-income household are fully subsidized by the government. For the employed, the total insurance premium is typically 4.6 per cent of their wages (Underwood, 2009). as well, the taxes from tobacco excise tax and the national lottery revenues are injected/infused into the system (Bureau of National Health Insurance, 2010).

The cost of the services from providers is covered mainly through reimbursements from the NHI. but it is also partially covered by co-payments from users (Cheng, 2003). The NHI is also supplemented by a co-insurance system where the user pays a nominal co-payment to the health care provider upon the use of its services. Its purpose is to discourage overuse. This may be compared to how wait times stemming from the referral-system in Canada discourages unnecessary hospital visits. The co-payment is usually a few dollars, or a fraction of the true cost of the service provided. The amount is capped by the NHI to eliminate any concerns of bankruptcy resulting from an accumulation of the fees. It is also waived for catastrophic diseases, individuals from low-income households or remote areas, infants and veterans.

One problematic area of health care that the NHI has tackled progressively is implementing the universal coverage and assuring similar health status between the indigenous and marginalized populations, and the rest of Taiwan. In order to eliminate disparities regarding access to health care, NHI has approached both the demand and supply side. On the demand side, it ensured that the population at risk were provided with insurance, and exempted them from co-payment. On the supply side, it has implemented an Integrated Delivery System (IDS), and guaranteed income for physicians practicing in remote areas (Bureau of National Health Insurance, 2010). Although certain disparities still exist, policy tools such as IDS and rural payment bonuses contribute to continuous improvements (Chou, Huang et al. 2004).

Another innovation is the integration of traditional methods in a modern system. As traditional Chinese medical practice is an accepted form of medicine, and is a mainstream medical care in Taiwan. Chinese medicine is insured under the NHI. Traditional Chinese Medical (TCM) services ranges from acupuncture and fire cupping massages to medicinal herbs. It is believed to be effective in alleviation of many illnesses and disease, managing pain and promoting well-being. Traditional Chinese medicine is often used in conjunction with Western biomedicine (Chen, Chen et al. 2007) and accounts for six per cent of health expenditure on outpatient services in Taiwan (Bureau of National Health Insurance, 2010). However, not all TCM clinics are registered under the NHI, and standardization regarding the quality was not so straightforward.

As it turns out, the NHI began facing deficits in the late 1990s, relying on bank loans to pay health care providers. Between 1996 and 2009, NHI expenditures grew at an average of 5.27 per cent a year, exceeding NHI revenues with an average growth rate of 4.02 per cent a year (Bureau of National Health Insurance, 2010). The exceeding expenditures were a fault of the open-ended health insurance system relying on a Fee-For-Service (FFS) payment of the providers. The health care providers performed unnecessary procedures  and prescribed unnecessarily expensive. drugs at the expense of the NHI. Submission of false reimbursement claims was another example of misuse  of the system (Cheng 2003).

Due to the competitive nature of FFS, physicians were called upon to see an overwhelmingly large volume of patients per day, leading to rushed visits and insufficient time to get a complete patient history or conducting a thorough exam, which could lead to misdiagnosis, improper treatment or delays in proper treatment. This led to a vicious cycle of doctors ordering frequent follow-ups, which contributed to higher patient volumes and shorter visits. Moreover, many patients were led to believe/feel that their problems were not adequately addressed, resulting in repeat visits and 'doctor shopping' – visiting numerous practitioners simultaneously, and seeking unnecessary care, or care that does not require specialists. all further impinging on the system (Gunde, 2004).

To address some of these issues, the NHI made a number of changes in how the health care providers were reimbursed. From 1998 to 2002, a global budget policy was imposed on different sectors, replacing the Fee-for-Service system. The Global policy set an expenditure cap for each sector, whereby services provided beyond the cap would be reimbursed at lower rates. The new policy incentivized health care providers to stay within their set budget. Global budgeting proved to be effective, and overall growth rates of per capita medical spending declined in nearly all of the health sectors in the early 2000s. However, it was an incomplete solution as the NHI continued to face ever increasing expenditures.

In 2004, the NHI implemented a Resource-Based Relative-Value Scale (RBRVS) into the physician fee schedule, where physicians were paid according to the "relative value" of services provided and the resources they consumed. It is based on the amount of physican-involving work that goes into the service, the practice expense associated with the service, and the professional liability expense for the provision of that service; also being adjusted according to the geographic region (American Association for Pediatrics, 2005).

The NHI continues to experiment with different methods of payment of provider. The most recent change to the heatlh care system was in 2010, where the NHI introduced a diagnosis-related-group reimbursement (DRG) scheme to pay physicians. Under this scheme, the physicans are reimbursed at a certain rate for different types of patients according to their primary diagnosis (Bureau of National Health Insurance, 2009).

Further efforts to improve the quality of the NHI system led to the introduction of the IC (Integrated Circuit) Smart Card: a mandatory health card of sorts, but integrating innovative information technology.  The Smart Card contains electronic data about the cardholder's personal identity, medical record, prescription history, remarks for catastrophic diseases, number of visits, administrative and expenditure information among other things (Smart Card Alliance, 2005). The introduction of the Smart Card in 2002, had allowed Taiwanese hospitals and clinics to send electronic records on a daily basis to the Bureau of NHI, where the data is analyzed and audited on a regular basis. The Smart Card makes it possible to monitor high-utilization cases through patient profile analysis; prevent fraud from aberrant medical claims; and keeps surveillance of public hazards, tracking down suspects of communicable disease (Bureau of National Health Insurance, 2009).

The tracking of symptoms of communicable diseases is becoming increasingly important with the rise of pandemic disease, where persons infected must be identified and isolated as soon as possible to prevent the spreading of the infection. Although it is a relatively new system, preliminary results have indicated that the Smart Card has enormous potential to be a key tool in reducing infectious outbreaks, such as severe acute respiratory syndrome (SARS), through implementation of an on-line real-time mechanism for disease control, tracking and surveillance (Huang and Hou 2007).

Another major benefit from the use of Smart Card technology is the reduction in administrative costs due to improved administrative, billing and provider efficiencies. The technology has allowed for automatic operation of electronic transfer of medical records and bills, resulting in expedited reimbursements of providers. As the Smart Cards last for several years, it has also eliminated costs involved with frequent replacement of older health cards, which were previously made of non-durable material. As a result, Taiwan's health care system has the lowest administrative costs in the world, accounting for only two per cent of its total health expenditure. Comparatively, Canada spends 16 per cent of total health expenditures on administration and the United States spends 31 per cent (Woolhandler, 2003). The low administrative cost significantly contributes to how Taiwan has maintained the low rate of health expenditure spending over the accumulated GDP spending.

In spite of these efforts of new innovations and policy implementation, health care costs are still rising in Taiwan. The NHI's deficit is expected to reach $3.2 billion US dollars by the end of 2010 if effective measures are not put into place. The government could increase spending from its GDP by raising the premiums although it would cause public unrest in the process. But even so, the extra income generated from increased premiums will only be a temporary measure in keeping the balance and offsetting the existing deficit of $1.84 billion dollars US (Taiwan Today, 2010).

Taiwan is now looking overseas for other potential solutions. Medical tourism is a new and growing area in the world economy (Morgan, 2009) and it has come to the attention of the Taiwanese health care industry. In hopes of easing its growing deficit and financial burden, the Taiwanese government's Department of Health began planning distribution channels and marketing campaigns on medical tourism. Now, Taiwan brands itself as a home for first-rate medical care services (International Medical Tourism Journal, 2009). Taiwan has long been popular with its expatriate population as a medical-travel destination (Tung, 2010). However, the market is expected to expand by several folds as Taiwan further opens its door to mainland China. With the recent lift of travel restrictions, 2009 alone brought 40,000 visitors from China to Taiwan to undergo health checkups and cosmetic surgery (Kastner, 2010).

Creating a system that is both financially sustainable and meets the needs of an evolving population is a fine balancing act with many factors. Taiwan will face health care challenges common to many other countries in the near future: an aging population; rising cost of the workforce in the medical health industry; and increasing costs of new technology and drug research and development.

The two weeks I spent in Taiwan taught me that there are no easy tricks to finding a solution to a problem. The development of the health care system is a continually evolving process that is sensitive to time, place, political and economic state of the country, and the needs of the people.

As it stands, the Taiwanese government is currently working on a 'second generation' NHI reformation, implementing new policies and strategies to make the health care system more sustainable (Bureau of National Health Insurance, 2010). Collaborating with other nations by sharing information on policy implications, research data, consultations and other innovations have led to the development and establishment of what is the NHI today. Further innovation and collaboration among nations can ensure that future steps taken to develop and to implement health care policies are more effective.

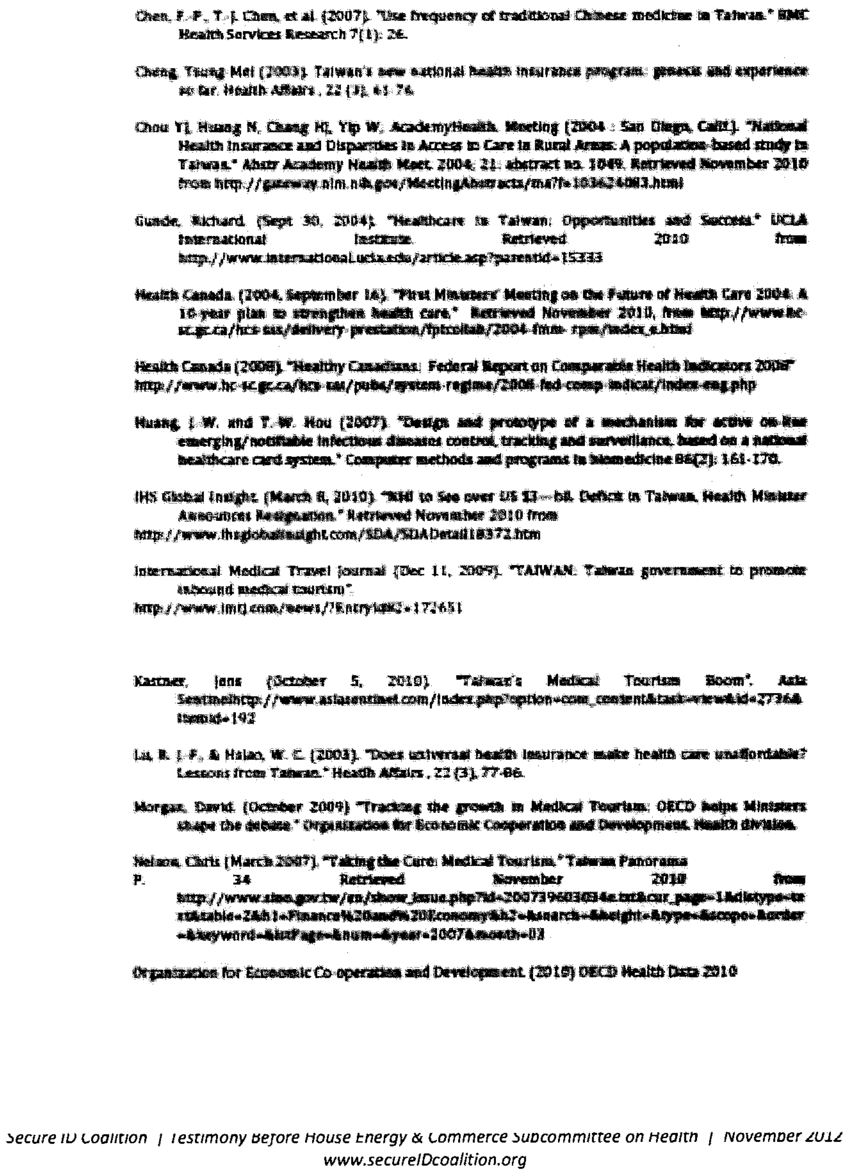
For now, Taiwan and the NHI stands as a successful case of how a nation was able to successfully established a universal health care coverage for the entire nation – almost from ground up. The system offers, at an affordable cost to the users, easy access to comprehensive health care of high quality. Despite some of the financial weaknesses it has shown and the downfalls it has faced in the last fifteen years, it is an example of how a government can strategically manage its resources in order to serve its people effectively; providing access to health care to those who need it most.

## References

American Academy of Pediatrics (2008) "Application of the Resource-Based Relative Value Scale System to Pediatrics".
http://aappolicy.aappublications.org/cgi/reprint/pediatrics;122/6/1395.pdf

Bureau of National Health Insurance (2010). "National Health Insurance in Taiwan".
http://www.nhi.gov.tw/webdata/AttachFiles/2010%96profile_990501.pdf

Central Intelligence Agency. (2010, Nov). Taiwan. Retrieved November 2010, from The World Factbook: https://www.cia.gov/library/publications/the-world-factbook/geos/tw.html



Chen, F.-P., T.-J. Chen, et al. (2007). "Use frequency of traditional Chinese medicine in Taiwan." BMC Health Services Research 7(1): 26.

Cheng, Tsung-Mei (2003). Taiwan's new national health insurance program: genesis and experience so far. Health Affairs , 22 (3), 61-76.

Chou YJ, Huang N, Chang HJ, Yip W, AcademyHealth. Meeting (2004 : San Diego, Calif.). "National Health Insurance and Disparities in Access to Care in Rural Areas: A population-based study in Taiwan." Abstr Academy Health Meet. 2004; 21: abstract no. 1049. Retrieved November 2010 from http://gateway.nlm.nih.gov/MeetingAbstracts/ma?f=103624083.html

Guade, Richard. (Sept 30, 2004). "Healthcare in Taiwan: Opportunities and Success." UCLA International Institute. Retrieved 2010 from http://www.international.ucla.edu/article.asp?parentid=15333

Health Canada. (2004, September 16). "First Ministers' Meeting on the Future of Health Care 2004: A 10-year plan to strengthen health care." Retrieved November 2010, from http://www.hc-sc.gc.ca/hcs-sss/delivery-prestation/fptcollab/2004-fmm-rpm/index_e.html

Health Canada (2008). "Healthy Canadians: Federal Report on Comparable Health Indicators 2008"
http://www.hc-sc.gc.ca/hcs-sss/pubs/system-regime/2008-fed-comp-indicat/index-eng.php

Huang, J. W. and T. W. Hou (2007). "Design and prototype of a mechanism for active on-line emerging/notifiable infectious diseases control, tracking and surveillance, based on a national healthcare card system." Computer methods and programs in biomedicine 86(2): 161-170.

IHS Global Insight. (March 8, 2010). "NHI to See over US $1—bn Deficit in Taiwan, Health Minister Announces Resignation." Retrieved November 2010 from
http://www.ihsglobalinsight.com/SDA/SDADetail18372.htm

International Medical Travel Journal (Dec 11, 2009). "TAIWAN: Taiwan government to promote inbound medical tourism".
http://www.imtj.com/news/?EntryId82=172651

Kastner, Jens (October 5, 2010). "Taiwan's Medical Tourism Boom". Asia Sentinelhttp://www.asiasentinel.com/index.php?option=com_content&task=view&id=2736&Itemid=192

Lu, R. J.-F., & Hsiao, W. C. (2003). "Does universal health insurance make health care unaffordable? Lessons from Taiwan." Health Affairs , 22 (3), 77-86.

Morgan, David. (October 2009) "Tracking the growth in Medical Tourism: OECD helps Ministers shape the debate." Organization for Economic Cooperation and Development. Health division.

Nelson, Chris (March 2007). "Taking the Cure: Medical Tourism." Taiwan Panorama
P. 34 Retrieved November 2010 from http://www.sino.gov.tw/en/show_issue.php?id=200739603034e.txt&cur_page=1&distype=text&table=2&h1=Finance%20and%20Economy&h2=&search=&height=&type=&scope=&order=&keyword=&lstPage=&num=&year=2007&month=03

Organization for Economic Co-operation and Development. (2010) OECD Health Data 2010

Reid, T.R. (2008). Taiwan Takes Fast Track to Universal Health Care. NPR. http://www.npr.org/templates/story/story.php?storyId=89651916

Smart Card Alliance. (2005). "The Taiwan Health Care Smart Card Project". http://www.smartcardalliance.org/resources/pdf/Taiwan_Health_Card_Profile.pdf

Statistics Canada (2008) Healthy Canadians: A Federal Report on Comparable Health Indicators 2008

Taiwan Today (March 9, 2010) Health minister resigns over health premium increase http://www.taiwantoday.tw/ct.asp?xItem=95660&CtNode=414

Tsang IK. Establishing the efficacy of traditional Chinese medicine. Nat Clin Pract Rheumatol 2007;3:60-1.

Tung, Sarah (July 16, 2010). "Is Taiwan Asia's New One-Stop Plastic Surgery Shop?". http://www.time.com/time/world/article/0,8599,2004023,00.html#ixzz0u6ep3Q9x

Underwood, Anne (Nov 3, 2009). "Health Care Abroad: Taiwan". The New York Times. http://prescriptions.blogs.nytimes.com/2009/11/03/health-care-abroad-taiwan/?scp=4&sq=hsiao%20taiwan&st=cse
IHS Global Insight

Zuellig Pharma (2006). "The expansion of medical tourism in Asia is proving a healthy boost for a growing number of the region's economies." The Market Partners. Issue 33. pg 8-9.

Mr. PITTS. The Chair thanks the gentleman and now recognizes Mr. Terzich for 5 minutes for an opening statement.

## STATEMENT OF MICHAEL H. TERZICH

Mr. TERZICH. Thank you, Mr. Chairman, Ranking Member Pallone, and members of the subcommittee. My name is Michael Terzich, and I am the senior vice president of global sales and marketing for Zebra Technologies Corporation, which is headquartered outside of Chicago in Lincolnshire, Illinois.

I greatly appreciate the opportunity to testify today and share my company's perspective on how secure ID card technology can help address the problem of fraud, waste, and abuse in the healthcare system and, more specifically, the Medicare program.

My company commends you, Mr. Chairman, along with Ranking Member Pallone, for your leadership on this issue. We likewise wish to express our appreciation to your colleague from our home State of Illinois, Congressman John Shimkus, who has worked diligently——

Mr. PITTS. Could you pull your microphone a little closer to you? Thank you.

Mr. TERZICH [continuing]. Who has worked diligently on this issue and has been a key leader in efforts to eliminate healthcare and Medicare fraud.

As a global leader in the secure ID digital printer industry, Zebra designs and manufactures a variety of products that use sophisticated technology to safeguard identity and streamline business processes. As a result, I will focus my remarks on H.R. 2925, the Medicare Common Access Card Act, which, as you know, would establish a pilot program to test the potential security benefits associated with modernizing Medicare through the use of secure ID card technology.

Zebra believes that this kind of technology will help protect the continued integrity of the Medicare program. Our confidence reflects the fact that technology enjoys a strong record of performance in both the Federal Government and the private sector. From the Department of Defense's use of secure identity credentials for logical and physical access to vital defense facilities and data networks, to the work of global credit card companies in advancing combined Chip and PINsystems which protect the integrity of both personal identity and financial transactions, secure ID technology provides a tested platform that Medicare can leverage in advancing efforts to combat fraud, waste, and abuse.

Moreover, our experience in the private sector is that the digitization of business processes within Medicare will also help reduce the overall cost of operating the Medicare system. On this point, we associate ourselves with the testimony from our colleagues in the Secure ID Coalition, who address this point in greater detail in their statement.

Let me briefly turn to three key technical elements of secure identification that the subcommittee may wish to consider as it advances H.R. 2925.

The first is the value of leveraging the experience the Federal Government has gained over the past decade in improving identity security. In particular, we believe that the Federal Information

Processing Standard Publication 201, better known by its acronym FIPS 201, and its subsidiary standards known as Personal Identity Verification 1, Personal Identity Verification 2, and Personal Identity Verification Interoperable, also known by their acronyms, PIV–1, PIV–2, and PIV–I, provide a proven framework for providing secure identity management technology into the fight against Medicare fraud.

Since 2005, the Federal Government has issued millions of FIPS 201 and standard PIV cards to Federal employees and contractors covering a wide range of trusted identity applications. Given the Federal Government's significant and positive experience in using PIV-based secure ID technology elsewhere, we believe it makes sense to employ the FIPS 201 standard in the pilot program that is created by H.R. 2925.

Second is the recognition of the value that secure ID card technology brings to the fight against counterfeiting and identity theft. Counterfeiting secure ID cards is exponentially more difficult than counterfeiting paper-based cards, even for the most sophisticated, well-financed criminal enterprises. This enhanced security comes from a combination of media features, printer capabilities, and coding of encrypted data on the smart chip database verification, and secure methods and processes. H.R. 2925's pilot program will provide an opportunity to test these features and determine the best combination for the Medicare system.

Third, Mr. Chairman, both security and efficiency are substantially enhanced through the use of a decentralized print model, which provides a realtime tie between the creation of a secure ID card and the immediate verification of the cardholder's information. Delays or gaps in time between these two steps, which inevitably occur when cards are manufactured in a remote centralized manner, increase opportunities that can be otherwise reduced through the use of a decentralized print model.

In sum, Mr. Chairman, secure ID card technology enables the use of tested security features which enhance privacy and identity protection. PIV-compliant secure ID cards provide secure, multifactor authentication at a high level of assurance by combining cryptographic private authentication with a personal identification number in a durable, tamper-resistant card format. Once a secure ID card is programmed and associated with a user, it provides a trusted, authentical identity usable for a wide range of cyber-based and physical transactions.

Thank you again, Mr. Chairman, for the opportunity to testify today. We stand ready to assist the subcommittee in developing legislative language related to the technical issues I have mentioned and urge the subcommittee to report out H.R. 2925 with modifications early next year. I look forward to any questions you or your colleagues may have.

[The prepared statement of Mr. Terzich follows:]

STATEMENT OF
MICHAEL H. TERZICH
SENIOR VICE PRESIDENT, GLOBAL SALES AND MARKETING
ZEBRA TECHNOLOGIES CORPORATION

BEFORE THE SUBCOMMITTEE ON HEALTH
COMMITTEE ON ENERGY & COMMERCE
U.S. HOUSE OF REPRESENTATIVES

ON "EXAMINING OPTIONS TO COMBAT HEALTH CARE
WASTE, FRAUD AND ABUSE"

WEDNESDAY, NOVEMBER 28, 2012

## Statement Highlights

- Secure ID technology can help significantly reduce the fraud, waste and abuse within the health care system and, more specifically, the Medicare program. It will also aid Medicare by reducing the transaction costs associated with managing the program.
- The Federal Information Processing Standard Publication 201 (FIPS 201) provides a tested framework for bringing secure identity management technology into the fight against health care and Medicare fraud. Leveraging existing FIPS 201 standards will help ensure that the pilot is secure, easy to rollout and adopted by both beneficiaries and providers.
- Counterfeiting secure ID cards is exponentially more difficult than counterfeiting paper-based cards. This enhanced security comes from a combination of media features, printer capabilities, encoding of encrypted data on to the smart chip, database verification and secure methods and processes.
- Both security and efficiency are substantially enhanced through the use of a decentralized print model which provides a concurrent, real-time tie between the creation of a secure ID card and the immediate verification of the cardholder's information.

## Full Statement

Introduction

Thank you, Mr. Chairman, Ranking Member Pallone and members of the Subcommittee. My name is Michael Terzich and I am the Senior Vice President of Global Sales and Marketing for Zebra Technologies Corporation, which is headquartered outside of Chicago in Lincolnshire, Illinois.

I greatly appreciate the opportunity to testify today and share my company's perspective on how secure ID card technology can help address the problem of fraud, waste and abuse in the health care system and, more specifically, the Medicare program.

My company commends you, Mr. Chairman, along with Ranking Member Pallone, for your leadership on this issue. We likewise wish to express our appreciation to your colleague from our home state of Illinois, Congressman John Shimkus, who has worked diligently on this issue and has been a key leader in efforts to eliminate health care and Medicare fraud.

As a global leader in the secure ID digital printer industry, Zebra designs and manufactures a variety of products that use sophisticated technology to safeguard identity and streamline business processes. As a result, I will focus my remarks on H.R. 2925, the Medicare Common Access Card Act, which, as you know, would establish a pilot program to test the potential security benefits associated with modernizing Medicare through the use of secure ID card technology.

Zebra believes that this kind of technology will help protect the continued integrity of the Medicare program. Our confidence reflects the fact that the technology enjoys a strong record of performance in both the federal government and the private sector. From the Department of Defense's use of secure identity credentials for logical and physical access to vital defense facilities and data networks to the work of global credit card companies in advancing combined chip and PIN systems which protect the integrity of both personal identity and financial transactions, secure ID technology provides a tested platform that Medicare can leverage in advancing efforts to combat fraud, waste and abuse.

Moreover, our experience in the private sector is that the digitization of business processes within Medicare will also help reduce the overall cost of operating the Medicare system. On this point, we associate ourselves with the testimony from our colleagues in the Secure ID Coalition, who address this point in greater detail in their statement.

Overall System Benefits

Zebra's products are used by governments and businesses to change processes, making them faster, easier, and more secure. Even the most dedicated employees may eventually err over long periods of time when processing multiple routine transactions. Automating the most mundane, data-centric portions of those tasks allows those employees to focus on the most important aspects of their job, while facilitating the collection of more data, more accurately, with more security. Our experience underscores that substantial cost savings result from this improved accuracy and further opportunities for improvement will arise as data for analysis is more readily available.

Consequently, we believe there will be substantial cost savings for Medicare arising from the use of secure ID technology – both through its ability to combat the waste, fraud and abuse within the current, paper-based Medicare card system and from the efficiencies and savings that will be gained through the digitalization of business processes within the Medicare system. Furthermore, additional savings will be garnered through the ability of secure ID card technology to reduce the incidence of identity theft from recipients and, thus, any consequential issues impacting Medicare personnel due to responding to beneficiaries, reissuing cards or investigating incidents.

As noted previously, we associate ourselves with the testimony of the Secure ID Coalition and understand that the Coalition's statement to the Subcommittee will address the issue of systemic cost savings issue in greater detail. Capturing all such savings takes on even greater urgency as Congress looks to balance the important public policy goals of reducing the deficit and providing health care to our nation's elderly.

Secure Credentialing has Strict Requirements

Secure identity management and verification starts with trusted credentialing technologies. Over the past decade, the federal government has made considerable progress in improving identity security. This experience positions Medicare to leverage the federal government's substantial investment in secure ID technology in the fight against Medicare fraud. This also enhances the effectiveness of back-end analytic tools and will enable enforcement efforts to be more specifically targeted to situations which data analysis indicates merit more thorough investigation.

One of the keystones in the effort to create trusted credentials in the federal government began on August 27, 2004, when then-President George W. Bush issued Homeland Security Presidential Directive 12 (HSPD-12). Created initially in response to terrorist threats, HSPD-12 directed the use of a common identification credential for both government employees and contractors that would govern both logical and physical access to federally-controlled facilities and information systems.[1]

Following this, the National Institute of Standards and Technology (NIST) created the Federal Information Processing Standard Publication 201 (FIPS 201) for secure and reliable forms of identification. The FIPS 201 requirement for physical and logical access for federal employees and contractors is defined by two stringent standards: Personal Identity Verification I and

[1] Homeland Security Presidential Directive/HSPD-12, Office of the Press Secretary, August 27, 2004. http://csrc.nist.gov/drivers/documents/Presidential-Directive-Hspd-12.html.

Personal Identity Verification II (PIV I and PIV II).[2] The PIV I and PIV II standards affect all secure ID cards designed for use in federal applications and require federal agencies to[3]:

- "Establish roles to facilitate identity proofing, information capture and storage, and card issuance and maintenance."
- "Develop and implement a physical security and information security infrastructure to support these new credentials."
- "Establish processes to support the implementation of a PIV program".

In addition to and following the creation of PIV I and PIV II, NIST created PIV-Interoperable (PIV-I) for use by other organizations that wish to issue secure credentials that are interoperable with the federal government standards.

Deployment of PIV continues to gain momentum. In fact, the federal government has issued millions of FIPS 201 standard PIV cards to federal employees and contractors since 2005 across a wide range of trusted identity applications.[4] Given the federal government's significant and

[2] The PIV I requirements define the control objectives and security requirements described in FIPS 201, including the standard background investigation required for all federal employees and long-term contractors. The PIV II standards define the technical interoperability requirements described in FIPS 201. More specifically, PIV II details the hardware implementation standards for implementing the identity credentials.

[3] "Privacy Impact Assessment for the Department of Justice Personal Identity Verification (PIV) Card System," U.S. Department of Justice, July 20, 2007.

[4] "Personal Identity Verification Interoperability (PIV-I) for Non-Federal Issuers: Trusted Identities for Citizens across States, Counties, Cities and Businesses," Smart Card Alliance, February 2011.

positive experience in using PIV-based secure ID technology elsewhere, we believe it makes sense to employ the FIPS 201 standards in the pilot program that is created by H.R. 2925. Using the current FIPS 201 standards will ensure security, simplify implementation, reduce costs and leverage both the experience and know-how of an existing industry and the federal government's significant investment in the existing infrastructure. As noted previously, the use of FIPS 201 PIV standards will likewise enhance anti-fraud enforcement activities as back-end analytics will be able to more precisely focus on areas of potential concern.

## The Importance of Secure ID Card Printers

Counterfeiting secure cards is exponentially more difficult than counterfeiting paper-based cards, even for the most sophisticated, well-financed criminal enterprises. Even if a criminal enterprise could gain access to a secure card printer, it would still have to reverse engineer the security system, obtain secure printing supplies, hack into the secure network, encode PIN or biometric data on the smart chip, print counterfeit cards and then use those cards to create fraudulent transactions – with all of that having to be done before the secure card printer was declared as missing. Even then, each fraudulent transaction would have a known identity which would speed the identification and investigation of subsequent transactions, making it more likely to capture the perpetrators quickly.

Overall, card security comes from a combination of media features, printer capabilities, database verification with encrypted data on the smart chip and secure methods and processes. To prevent counterfeiting, alteration or duplication, there are many techniques that can be used with digital printers. Images or information content can be printed on the card, stored in the chip on the card, or sent to a secure database. When using the information, the combination of data is checked to ensure authenticity.

Even if one of those datasets is compromised, the combination will be known to be invalid and a potential fraud can be more quickly identified. Furthermore, cards with pre-printed security features, including ultraviolet-visible text and graphics or unique on-demand printing capabilities, such as nano-taggant inks or laminate with holographic metallization, can be employed to make counterfeiting more difficult and to create multiple layers of security that allow providers, staff, investigators and law enforcement to identify counterfeit cards. H.R. 2925's pilot program will provide an opportunity to test these features and determine the best combination for the Medicare system.

A Decentralized, Print Model Is Essential

The pilot program contemplated by H.R. 2925 should include and reflect a decentralized print model as a way of further enhancing identity security. The advantages of a decentralized approach reflect the fact that security is enhanced when there is a concurrent, real-time tie between the creation of a secure ID card and the immediate verification of the cardholder's information. Delays or gaps in time between these two steps – which inevitably occur when cards are manufactured in a remote, centralized manner – increase opportunities for fraud that can be otherwise reduced through the use of a decentralized print model.

Consequently, we urge that the pilot program focus on using a model of real-time production of secure ID cards that concurrently verifies a patient's or provider's identity and qualifying status. This will enhance personal accountability and streamline processing, allowing Medicare officials to focus on accuracy and security rather than unproductive processing steps. It will also reduce opportunities for criminals to divert or intercept the card or any corresponding identification documents. By leveraging well-established authentication processes, card security standards, and secure data processing networks, this important enrollment process can be implemented quickly and securely.

## Conclusion

When used in a properly implemented system, secure ID card technology enables the use of tested security features which enhance privacy and identity protection. PIV-compliant secure ID cards provide secure, multi-factor authentication at a high level of assurance by combining a cryptographic private authentication with a personal identification number in a durable, tamper-resistant card format. Once a secure ID card is programmed and associated with a user, it provides a trusted, authenticable identity usable for a wide range of cyber-based and physical transactions.

Thank you, again, Mr. Chairman, for the opportunity to testify today. We stand ready to assist the Subcommittee in developing legislative language related to the technical issues I have mentioned and urge the Subcommittee to report out H.R. 2925, with modifications, early next year. I look forward to any questions you or your colleagues may have.

Mr. PITTS. The Chair thanks the gentleman and now recognizes Dr. Fu for 5 minutes for an opening statement.

## STATEMENT OF KEVIN FU

Mr. FU. Good morning, Chairman Pitts, Ranking Member Pallone, and distinguished members of the subcommittee. Thank you for the invitation to testify on the expectations of smart cards to combat waste, fraud, and abuse in the Medicare program.

My name is Kevin Fu. I teach courses on smart cards and how to build secure computer systems in health care. While studying at MIT 17 years ago, I helped a hospital deploy a smart-card precursor to authenticate healthcare providers. My responsibility included issuing replacement authentication cards to nurses and physicians who would lose their cards. I am speaking today as an individual.

While smart cards may reduce fraud in other sectors, there do remain challenges that may make deployment more costly and less effective than anticipated. One, smart cards authenticate smart cards, not people. The cards can still be borrowed or stolen. Two, there are several hacks against smart cards that have led to fraud and cloned credentials. And three, interrupting the clinical workflow can lead to unanticipated consequences on patient care that need to be investigated.

So let me highlight the types of fraud remaining in healthcare programs in other countries who have already deployed smart cards for their national health programs. Further details do appear in my written testimony.

In France, it was routine for people to share smart cards. Many healthcare professionals still do not have the smart-card readers after nearly 15 years. In such cases, a patient in France uses an ancient paper-based system for reimbursement. Thus, loopholes remain for fraud, and the French maintain two separate payment processing systems.

In Taiwan, fraud persists because multiple patients collude with one or more doctors to report higher examination and medication fees such that they can split the extra money among themselves. Even a secure smart card cannot stop that kind of fraud.

In Germany this past summer, the smart-card deployment proved difficult when the manufacturer accidentally distributed cards without PINs to 2 million patients. All the smart cards required replacement.

In Britain, a survey found that general practitioners and staff share their National Health Service smart cards despite warnings of disciplinary action.

And in Australia, they recently terminated its $25 million contract last month for their national eHealth program using a smart-card authentication service.

Mr. FU. Let me also highlight a few security shortcomings in smart cards just to give you an idea of what could be expected.

In 2011, the DOD Common Access Card was suggested as a model approach for the Medicare Common Access Card. This was a valid approach. But 2 months later, a Chinese computer virus hacked into the computers connected to smart-cards readers to steal PINs from the military cards.

Security, I teach my students, is very difficult to measure or predict and a common property of the hacked smart-card system is that the smart-card system was previously believed to be secure.

In 2006, I culled out a study that analyzed the security of credit cards containing contact-less smart-card technology. The New York Times reported that card companies imply through their marketing that the data was encrypted to make sure that a digital eavesdropper could not get any intelligible information. But instead we found that we could wirelessly scan the credit cards through clothing with a tiny device built with $150 in spare parts.

The Chip and PIN system deployed overseas has also experienced several security flaws that led to fraud. The BBC reported that cards were found to be open to a form of cloning despite past assurances from banks that Chip and PIN could not be compromised. Hundreds of Chip and PIN machines in stores and supermarkets across Europe have been tampered with to relay credit card data to overseas fraudsters to make cash withdrawals.

With implications to public health, my understanding is that a significant source of fraud comes from home healthcare services. A home healthcare patient who cannot remember to eat breakfast on his own is not going to be able to remember a PIN or password. A stroke victim who must relearn how to swallow may not be able to talk or feed herself without assistance. The home healthcare patient depends greatly on the kindness of others and can be particularly vulnerable to overly trusting a provider.

In short, a vulnerable home healthcare patient would likely comply with an unscrupulous provider who asked to hold onto the card and PIN so as not to inconvenience the patient.

I have four recommendations.

A pilot study should include a security analysis and penetration testing of the system by a neutral third party as well as tests designed with clinical engineers and health IT specialists to measure the impact on patient care.

Two, a pilot study should measure fraud in comparison with alternatives.

And three, a smart-card pilot should measure the impact on fraud while controlling for fraud reductions due to other fraud detection systems.

And four, there should be a period of public feedback coordinated by a neutral third party who has no financial interest in the outcome of the selected technology. NIST may be a logical choice, given that the proposed legislation refers to NIST standards.

So thank you. Let me conclude. And I am happy to answer any questions you may have.

Mr. PITTS. The Chair thanks the gentleman.

[The prepared statement of Mr. Fu follows:]

STATEMENT OF PROF. KEVIN FU, PH.D.

DEPARTMENT OF
ELECTRICAL ENGINEERING & COMPUTER SCIENCE
UNIVERSITY OF MICHIGAN
ANN ARBOR, MI
AND
DEPARTMENT OF COMPUTER SCIENCE
UNIVERSITY OF MASSACHUSETTS AMHERST
AMHERST, MA

# ON THE EXPECTATIONS OF SMART CARDS TO REDUCE MEDICARE FRAUD

SUBMITTED TO THE
SUBCOMMITTEE ON HEALTH
COMMITTEE ON ENERGY AND COMMERCE
UNITED STATES HOUSE OF REPRESENTATIVES

HEARING ON
EXAMINING OPTIONS TO COMBAT HEALTH CARE
WASTE, FRAUD AND ABUSE

WEDNESDAY, NOVEMBER 28, 2012

## Introduction

Good morning, Chairman Pitts, Ranking Member Pallone, and distinguished members of the Subcommittee. Thank you for the invitation to testify on the expectations of smart cards to combat waste, fraud and abuse in the Medicare program.

My name is Kevin Fu. I am an Associate Professor in Computer Science & Engineering with appointments at the University of Michigan and University of Massachusetts Amherst. My research investigates how to increase cybersecurity for systems ranging from smart cards to medical devices. My educational qualifications include a Ph.D., master's degree, and bachelor's degree from M.I.T.'s Department of Electrical Engineering and Computer Science. I serve on the NIST Information Security and Privacy Advisory Board, a Federal Advisory Committee, to identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy in Federal Government information systems. My industrial experience in software systems includes past employment at Cisco Systems, Microsoft, Hewlett-Packard, and the Information Systems department at Holland Community Hospital.

Experiences in smart card security and health care provide me with a broad perspective on risks and benefits of deploying information security technology in health care settings:

- My cybersecurity research includes the security analysis of contactless "smart card" credit cards ("Researchers See Privacy Pitfalls in No-Swipe Credit Cards," NY Times, October 23, 2006) showing how to wirelessly lift credit card numbers, card holder names, and expiration dates from smart cards protected with the highest levels of industry standard encryption—even through wallets and clothing[1]. I have given invited talks on the benefits and risks of smart card technology at conferences, universities, companies, various Federal Reserve Banks, the Federal Trade Commission, and the Toronto Police Fraud Squad.
- I am also known for research that analyzed the security of an implantable cardiac defibrillator—demonstrating that the device could be wirelessly tricked into inducing a fatal heart rhythm ("A Heart Device Is Found Vulnerable to Hacker Attacks," NY Times, March 12, 2008)[2].

[1] http://rfid-cusp.org/

[2] http://secure-medicine.org/

- I manufacture an experimental smart card for advanced security research at universities, industrial research labs, and the Department of Defense[3].
- At a community hospital, I participated in the roll out of a smart-card precursor to authenticate health care providers for accessing paperless medical records and an electronic billing system. The less exciting part of my job involved issuing replacement authentication cards to nurses and physicians who lost their cards.

I am speaking today as an individual. All opinions, findings, and conclusions are my own and do not necessarily reflect the views of HHS, NSF, or any of my past or present employers.

## Smart cards

Smart cards are math in plastic. I like math. The security depends on (1) how the cards are used in a system, (2) the difficulty of breaking various algorithms, and (3) the difficulty or tampering with the physical card. A flaw in any these three elements makes a smart card vulnerable. The first element is most relevant to Medicare fraud, and is often the weakest link in the chain.

While smart cards may reduce fraud in other sectors, there remain challenges that may make deployment more costly and less effective than anticipated:

1. Smart cards authenticate smart cards, not people. For this reason, a key shortcoming of even the most perfect smart card is the difficulty of securely linking the card with a person. Linking people to a smart card is notoriously difficult.
2. There are several documented hacks against smart cards.
3. Smart card hacking will lead to increased malware on clinical computing systems.
4. Interrupting clinical workflow can lead to unanticipated consequences on patient care.

My testimony summarizes general security problems in smart cards, fraud remaining in health care programs in other countries already using smart cards, and implications for public health.

[3] http://spqr.cs.umass.edu/moo/

## Problems with Smart Card and Payment Terminal Security

Below I highlight a number of security shortcomings in smart cards that led to card cloning and fraud for payments and facility access control. A common property is that the cards were seen as ironclad secure until they were not.

**Chinese hack of DoD Common Access Cards.** Authentication and identity systems that seem to work securely one day can lose that sense of security the next. For example, the DoD Common Access Card (CAC) was rightly cited as not having any problems with counterfeiting in 2011.

> "The Medicare Common Access Card Act of 2011 seeks to replicate the smart card technology currently used by members of our armed services and applies it to the Medicare system. The Department of Defense has issued over 20 million of these secure smart cards to authenticate and verify users for access to military programs and facilities. To date, DoD reports not a single Common Access Card has been counterfeited. We believe that seniors should benefit from the same identity security as members of our military." ("A smart approach to Medicare reform," The Hill, November 11, 2011)[4]

The DoD CAC was suggested as a model approach for the Medicare Common Access Card. Two months later, a Chinese computer virus hacked into the computers connected to smart card readers to steal PINs from DoD smart cards. The attack installed keyloggers by tricking personnel into viewing an emailed PDF file containing an exploit [5] ("New Sykipot variant can steal PINs from DoD smart cards," GCN, January 13, 2012). Security is very difficult to measure or predict; a common property of a hacked smart card system is that the smart card system was previously believed to be ironclad secure.

> "A Chinese-based cyber attack is targeting the Defense Departments Common Access Cards with technology that could steal information from military networks while troops

[4] `http://thehill.com/blogs/congress-blog/healthcare/191277-a-smart-approach-to-medicare-reform`

[5] One may wish to avoid viewing submitted testimony in a vulnerable PDF reader.

> and civilians work at their desks" ("Chinese virus targets DoD Common Access Card," ArmyTimes, January 18, 2012)[6]

**Breaking into government buildings protected with smart cards.** In 2006, Jonathan Westhues demonstrated the ease with which state lawmakers' smart cards for building access could be read and cloned[7]. He successfully read and cloned the ID card of California State Assembly member Fran Pavley, who remarked, "All that was done within a moment's notice of time without me even being aware of it."

**Contactless credit cards hack.** In 2006, I co-led a study that analyzed the security of credit cards containing contactless smart card technology[8].

> "The card companies have implied through their marketing that the data is encrypted to make sure that a digital eavesdropper cannot get any intelligible information. American Express has said its cards incorporate 128-bit encryption, and J. P. Morgan Chase has said that its cards, which it calls Blink, use the highest level of encryption allowed by the U.S. government. ... But in tests on 20 cards from Visa, MasterCard and American Express, the researchers here found that the cardholders name and other data was being transmitted without encryption and in plain text. They could skim and store the information from a card with a device the size of a couple of paperback books, which they cobbled together from readily available computer and radio components for $150." ("Researchers See Privacy Pitfalls in No-Swipe Credit Cards," NY Times, 10/23/2006)[9]

Whenever I meet a cashier with a contactless smart card reader, I ask how often customers use a contactless smart card. So far, the answer has consistently been none except for one cashier who said that the engineer who installed the reader tested a card. One cashier asked me to explain what the smart card reader did. Thus, fraud is likely low due to moderate levels of use and exposure.

[6] http://www.armytimes.com/news/2012/01/military-common-access-card-chinese-virus-011812w/

[7] http://www.yourtechtv.com/viewVideo.php?video_id=213&title=Cloning_RFID_Tags

[8] https://spqr.cs.umass.edu/publications.php?q=vulnerabilities

[9] http://www.nytimes.com/2006/10/23/business/23card.html

**Chip and PIN smart card hacks.** The Chip and PIN technology deployed overseas to protect credit cards is often heralded, but unfortunately this technology has also experienced several security flaws that led to fraud.

> "Cards were found to be open to a form of cloning, despite past assurances from banks that chip and PIN could not be compromised. ... For example, a physics professor...bought a meal for some people for 255 euros, and an hour and a half later, there were two withdrawals of 750 euros made from a nearby cash machine used by what appears to have been a clone of his card." ("Chip and pin weakness exposed by Cambridge researchers," BBC News, September 11, 2012)[10]

Many security vulnerabilities begin with complacency and a misbelief that lack of a reported security problem today means there can be no security problems tomorrow.

> "Dr Joel Brenner, the US National Counterintelligence Executive, warned that hundreds of chip and pin machines in stores and supermarkets across Europe have been tampered with to allow details of shoppers' credit card accounts to be relayed to overseas fraudsters. These details are then used to make cash withdrawals or siphon off money from card holders' accounts in what is one of the largest scams of its kind. ... An organised crime syndicate is suspected of having tampered with the chip and pin machines...." ("Chip and PIN scam has netted millions from British shoppers," The Telegraph, October 10, 2008)[11]

> "The devices were modified, by adding hardware, in order to send credit card details over mobile telephone networks to the scammers." ("Hundreds of tampered chip and PIN devices spread in stores across Europe," Softpedia, October 14, 2008)[12]

**Cloning proprietary smart cards.** Many smart cards are based on proprietary algorithms that have not been tested or evaluated with strong and open peer-review. Proprietary algorithms can

[10] http://www.bbc.co.uk/news/technology-19559124

[11] http://www.telegraph.co.uk/news/uknews/law-and-order/3173346/Chip-and-pin-scam-has-netted-millions-from-British-

[12] http://news.softpedia.com/news/Hundreds-of-Tampered-Chip-and-Pin-Devices-Spread-in-Stores-Across-Europe-95644.sl

lead to a false sense of security. For instance, this Dutch researcher shows how to clone a proprietary smart card in 5 seconds on an ordinary computer with $200 in parts.

> “With more than 300 million cards sold, HID iClass is one of the most popular contactless smart cards on the market. It is widely used for access control, secure login and payment systems. ... These cards are widely used in access control of secured buildings such as The Bank of America Merrill Lynch, the International Airport of Mexico City and the United States Navy base of Pearl Harbor. ... Other applications include secure user authentication such as in the naviGO system included in Dells Latitude and Precision laptops; e-payment like in the FreedomPay and SmartCentric systems; and billing of electric vehicle charging such as in the Liberty PlugIns system. iClass has also been incorporated into the new BlackBerry phones which support Near Field Communication (NFC). ... This attack, from beginning to end runs within 5 seconds on ordinary hardware.” (“Dismantling iClass and iClass Elite,” by Garcia et al. 17th European Symposium on Research in Computer Security (ESORICS 2012). Lecture Notes in Computer Science, Vol. 7459, 2012. Springer Verlag)[13]

**Barnes & Noble payment terminal hack.** Hackers increasingly target payment terminals.

> “Hackers have stolen credit card information for customers who shopped as recently as last month at 63 Barnes & Noble stores across the country, including stores in New York City, San Diego, Miami and Chicago, according to people briefed on the investigation. ... The information was stolen by hackers who broke into the keypads in front of registers where customers swipe their credit cards and enter their personal identification numbers, or PINs.” (“Credit card breach at Barnes & Noble stores,” NY Times, October 23, 2012)[14]

An attack that seemed farfetched a short time ago has become real. And the attack vector may have been a modified credit card containing a virus rather than a credit card number.

[13] http://www.cs.ru.nl/~rverdult/Dismantling_iClass_and_iClass_Elite-ESORICS_2012.pdf

[14] http://www.nytimes.com/2012/10/24/business/hackers-get-credit-data-at-barnes-noble.html

> "hackers installed malware on the so-called point-of-sale (POS) card readers to sniff the card data and PINs as customers typed them in. ... researchers installed their malware using a rogue credit card inserted into one device, which caused it to contact a server they controlled, from which they downloaded malware to the device." ("Thieves hack Barnes & Noble point-of-sale terminals at 63 stores," Wired, October 24, 2012)[15]

If a bookstore cannot protect its payment terminals from fraud, it is unlikely that a non-tech-savvy home health care worker can adequately protect a smart card reader carried from home to to car to home to use at "the point of service and use it to verify services received."

**Subway (sandwich) payment terminal hack.** Demonstrating that improper use of a card technology can render a payment system insecure, Subway sandwiches suffered a massive scam dating back three years undetected.

> "a band of Romanian hackers is alleged to have stolen payment card data from the point-of-sale (POS) systems of hundreds of small businesses, including more than 150 Subway restaurant franchises and at least 50 other small retailers. And those retailers made it possible by practically leaving their cash drawers open to the Internet, letting the hackers ring up over $3 million in fraudulent charges. ... The tools used in the crime are widely available on the Internet for anyone willing to take the risks, and small businesses' generally poor security practices and reliance on common, inexpensive software packages to run their operations makes them easy pickings for large-scale scams like this one, Marcus said." ("How hackers gave Subway a $3 million lesson in point-of-sale security," ArsTechnica, December 21, 2011)[16]

**Stealing data wirelessly from smart card terminals.** Hackers are getting more clever in how they exfiltrate data. Wireless exfiltration from a card reader is sufficiently common that Visa issued a warning to merchants.

[15] http://www.wired.com/threatlevel/2012/10/barnes-and-noble-pos-hack/

[16] http://arstechnica.com/business/2011/12/how-hackers-gave-subway-a-30-million-lesson-in-point-of-sale-security/

> "A new bulletin from Visa indicates that it is increasingly concerned about point of sale terminals being adapted to steal card data over Bluetooth connections. To combat this threat, Visa advises merchants to scan for Bluetooth signals, which could be evidence of a wireless skimming device transmitting stolen card numbers." ("Tampered card readers steal data via Bluetooth," American Banker, September 9, 2011)[17]

There is so much wireless traffic in a clinical environment, it would be extremely difficult and costly to effectively deploy wireless Bluetooth attack detectors at every smart card reader.

**Subway (Boston) smart card hack.** Several transit systems have suffered from hacks to the smart card payment process.

> "the students had uncovered vulnerabilities within the magnetic stripe and RFID card payment systems used for Boston Charlie Cards and Charlie Tickets. ... ("MIT Subway Hack Paper Published on the Web," PC Magazine, August 12, 2008)[18]

**Dutch transit smart card hack.** The Netherlands is home to several companies in the smart card industry. Unfortunately, the smart card system for transit payments was hacked.

> "The Dutch RFID public transit card, which has already cost the government $2B — no, that's not a typo — has been hacked even before it has been deployed. ... My guess is the system was designed by people who don't understand security, and therefore thought it was easy." ("Schneier on Security: Dutch RFID Transit Card Hacked," Schneier blog, January 21, 2008[19])

## International Problems with Smart Cards in National Health Programs

A number of countries already use smart cards for national health programs. One of the more interesting uses is to store a mini electronic health record on each card so that providers have in-

[17] http://www.americanbanker.com/security-watch/bluetooth-skimming-1042020-1.html

[18] http://www.pcmag.com/article2/0,2817,2327898,00.asp

[19] http://www.schneier.com/blog/archives/2008/01/dutch_rfid_tran.html

stant access to prescription data in emergencies and patients receive more consistent care across different providers ("Health care abroad: Taiwan," NY Times, November 3, 2009). Unfortunately, national health programs relying on smart cards for authentication continue to suffer from fraud and abuse. The articles below illustrate the types of problems one should not expect smart cards to solve in the Medicare program.

**France: Fraud and photographs.** In France, the "carte vitale" smart card has been in place since 1998. Until 2007, beneficiary cards did not include a photo[20]; it was routine for people to use other people's cards. In the French system, many health care professionals still do not have the smart card readers after nearly 15 years. In such cases, a patient pays the provider directly and instead uses an ancient paper-based system for reimbursement. Thus, loop holes persist for fraud. The French must maintain two separate payment processing systems.

> "Why launch a new version of the card? ... It is also open to fraudulent use." ("French carte Vitale to be upgraded," FrenchEntrée, 2006) [21]

A common source of smart card fraud happens during the vulnerable registration process. A secure smart card is much less effective against fraud if registration process remains weak.

> "Inadequate checks by social security authorities leave the system open to abuse by foreigners..." ("Calls to tackle carte Vitale fraud," The Connexion, May 5, 2009) [22]

> "Even if identity documents are becoming more and more secure...the requirements for obtaining these documents are particularly lax. ... it is easy to get a birth certificate for a borrowed identity or to counterfeit an identity. ... the carte Vitale is the object of massive fraud and there is no serious securitization process in place." ("France faces rise in identity fraud," Le Figaro, November 14, 2011) [23]

[20] N.B.: the proposed legislation in H.R. 2925 would also not include photos on beneficiary smart cards. However, including photos for the Medicare beneficiary demographic would likely prove infeasible to implement.

[21] http://www.frenchentree.com/france-lot-quercy-services-contacts/DisplayArticle.asp?ID=18469

[22] http://www.connexionfrance.com/news_articles.php?id=797

[23] http://plus.lefigaro.fr/note/france-faces-rise-in-identity-fraud-20111114-598540

> "The cards can also be used fraudulently, with the consent of the owner. Attempt to limit the phenomenon, all new cards issued Vitale since 2007 (about 15 million copies) include a photo. But the effectiveness of the measure - which apparently has never been evaluated - remains to be seen." ("Vitale card biometric expensive and difficult to implement," translated from Le Figaro, August 3, 2012)[24]

**Taiwan: Provider fraud and collusion.** The Taiwanese Bureau of National Health Insurance deployed a smart card system several years ago. While there are few reports of card cloning, more serious fraud persists because of collusion between patients and providers.

> "surgeons from the Taitung Hospital...fabricated medical records to claim subsidies from a Ministry of Health program to subsidize outpatient and inpatient service for intern physicians. ... supervisors...filed false medical record entries ... had also fabricated the visits of 36 patents" ("Prosecutors charge one surgeon, defer another in health insurance fraud case," The China Post, September 9, 2009)[25]

According to a security expert in Taiwan, multiple patients collude with one or more doctors to report higher examination and medication fees to the insurance payment system supervised by Bureau of National Health Insurance, such that they can split the extra money among themselves.

> "a former gynecologist ... allegedly performed surgeries on healthy patients, claiming more than NT$500,000 in reimbursements from the Bureau of National Health Insurance. He also gave patients chemotherapy to help them obtain tens of millions of dollars in insurance payouts." ("DOH to clamp down on health insurance fraud," Taipei Times, March 29, 2010)[26]

Even a secure smart card cannot stop this kind of fraud.

[24] http://www.lefigaro.fr/conjoncture/2012/03/08/20002-20120308ARTFIG00645-fraude-a-la-secu-sarkozy-veut-une-carte-vitale-biometrique.php

[25] http://www.chinapost.com.tw/taiwan/local/taitung/2009/09/09/223867/Prosecutors-charge.htm

[26] http://www.taipeitimes.com/News/taiwan/archives/2010/05/29/2003474144

**Germany: Fraud and ballooning costs.** After years of delay, Germany has spent its first billion of investment funds to issue smart cards (called Gesundheit) for its national health program ("Resistance to electronic health card: we do not have photos for you," translated from Süddeutsche.de, August 17, 2012).

> "The fraudulent misuse of health insurance cards caused billions in damage. ... The principle of the card cheater is easy: either several non-insured use a smart card together...or a group of relatives and friends in Germany. Sometimes the cards were also stolen from a deceased of those insured who have changed their policies, but have not yet returned the card." ("Smart card: Rip-offs by medical card," translated from Frankfurter Allgemeine, January 13, 2004)[27]

The deployment proved difficult when the smart cards were accidentally distributed without PINs.

> "Embarrassing mishap of the electronic health card: approximately two million patients have received faulty payment cards. The manufacturer promises to replace the defective copies quickly." ("Breakdown: Millions of faulty health payment cards," translated from Der SpiegelOnline, June 22, 2012)[28]

**UK: Providers sharing smart cards.** The British have discovered that general practitioners share their National Health Service smart cards.

> "A recent survey conducted by the GP's newspaper Pulse revealed that one in six NHS staff flouted the rules regarding confidential medical records, and shared smartcards. Despite CfH warnings that 'disciplinary procedures should follow' if smartcards are used improperly, 5% of GPs also admitted sharing their own smartcard." ("NHS loses contact to smartcards," Smartcard & Identity News, December 2008)[29]

[27] http://www.faz.net/aktuell/gesellschaft/kriminalitaet/chipkarten-abzocken-per-krankenkarte-1147791.html

[28] http://www.spiegel.de/wirtschaft/service/kassen-verschicken-elektronische-gesundheitskarten-ohne-pin-a-840405.html

[29] http://www.smartcard.co.uk/articles/NHSLosesContact.php

**Australia: Terminating smart card contract.** Australia is beginning to deploy smart cards for their national health program, but has run into snags in the USD$ 25M system.

> "IBM's AU$23.6 million contract with the National E-Health Transition Authority (NEHTA) is in tatters, and both sides have brought the lawyers in as the government implements an interim National Authentication Service for Health (NASH) system. ... IBM was tasked to develop a system that would use public key infrastructure and secure tokens, such as smart cards, in order to provide an authenticated service." ("Legal woes for IBM's e-health contract," ZDNet, October 25, 2012)[30]

## Implications for Public Health

**The overly trusting beneficiary.** My understanding is that a significant source of fraud comes from home health care services. A home health care patient who cannot remember to eat breakfast on his own is not going to be able to remember a PIN or password. A patient who qualifies for home health care can literally be home-bound. For instance, the patient might not be able to independently shop for groceries for over a year. A stroke victim who must relearn how to swallow may not be able to talk or feed herself without assistance. Thus, a home health care patient depends greatly on the kindness of others, and can be particularly vulnerable to overly trusting a provider. A vulnerable home care patient would likely comply with an unscrupulous provider who asks to "hold on to the smart card and PIN so as not to inconvenience the patient." In short, smart cards that work well for the subway traveller or retail shopper will likely not work as effectively for the demographic of home health care.

**Malware on clinical computing systems.** Because payment software for smart card readers are prone to targeted malware, requiring this software installed will increase the exposure of clinical computing systems to malware. How many systems will be exposed to malware? Over 1,058,469 Medicare physicians/suppliers billed Medicare last year.

[30] http://www.zdnet.com/au/legal-woes-for-ibms-e-health-contract-7000006359/

> "Computerized hospital equipment is increasingly vulnerable to malware infections, according to participants in a recent government panel. These infections can clog patient-monitoring equipment and other software systems, at times rendering the devices temporarily inoperable. ... malware at one point slowed down fetal monitors used on women with high-risk pregnancies being treated in intensive-care wards." ("Computer Viruses are Rampant on Medical Devices in Hospitals," MIT Technology Review, October 17, 2012)[31]

All hospitals struggle with reducing the amount of malware reaching their critical care systems. The malware often spreads via webmail accounts, networks—and USB sticks that circumvent all firewall controls. Medical device manufacturers often disallow the use of anti-virus products. Thus, clinical computing systems can suffer from severe consequences when infected with malware. Downtime can lead to delayed patient care (e.g., transporting seriously ill patients waiting for a time-critical angioplasty from a cath lab infected with malware that renders the surgical equipment unavailable) to faulty sensor readings. A cath lab is one USB stick away from a terminal connected to a smart card reader.

Because malware has spread from a chip and PIN smart card to the payment terminal, health care computing systems will likely become more vulnerable to malware that can steal or tamper with medical information.

## Questions

There are several questions on smart cards for Medicare that require more thought to find a meaningful answer.

1. Given that beneficiaries already share their paper cards, what would disincentivize these same beneficiaries from sharing a smart card and PIN?
2. How likely would a patient over 65 forget a smart card, give the smart card to a friend, or write the PIN on a sticky note and let a home health care provider hold on to the smart card?

[31] http://www.technologyreview.com/news/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals/

3. What is the clinical impact of introducing extra procedures to the critical path of the delivery of patient care if the card must be scanned "at the point of service and use it to verify services received by placing into a reader, entering their PIN, and confirming the transaction"? One of the greatest sources of medical errors leading to patient harm is a complicated clinical workflow. There could be benefits or risks, but the answer is unknown.

4. Who pays for the materials and time spent by health care professionals when a smart card vulnerability necessitates a reissuing of smart cards or smart card readers before the anticipated replacement date? What business will legitimate providers lose if the billing systems are unavailable or reverted to paper?

5. Who is responsible if a patient is harmed by malware spread to the clinical environment as a result of vulnerabilities in payment process software that connects to each smart card reader?

6. Who guards the guards? How bribable are the guards? When a smart card is lost, who has the authority to replace the card? In the case of the hospital where I worked, I had the authority to issue new cards to health care professionals. My salary at the time amounted to approximately $1\frac{1}{2}$ large pizzas per day.

## Recommendations

The expected benefits of smart cards need to take into account the full costs and risks shouldered by the non-fraudulent providers and beneficiaries. I would recommend the following:

1. A pilot study should include a security analysis and penetration testing of the system by a neutral third party, as well as tests designed with clinical engineers and health IT specialists to measure the impact on patient care.

2. A pilot study should measure fraud in comparison with alternatives. For example, it would be useful to know to what extent a less expensive photo ID would reduce fraud compared with

a smart card because other countries are increasingly adding photos to beneficiary cards to curb fraud[32].

3. A smart card pilot should measure the impact on fraud while controlling for fraud reductions due to fraud detection systems and strengthening of provider enrollment. That is, the smart card benefits should not be conflated with the benefits from other fraud reduction mechanisms.

4. There should be a period of public feedback coordinated by a neutral third party who has no financial interest in the outcome of the selected technology. NIST may be a logical choice given that the proposed legislation refers to NIST standards.

## Conclusion

It is important to reduce fraud, waste and abuse in the Medicare program. Given finite resources, does it make sense to invest in smart card infrastructure rather than better fraud detection systems? Rather than strengthening of provider enrollment? These questions are worth exploring, but the proposed pilot program does not explore such questions. Moreover, a pilot ought to account for the costs of time that health care professionals must spend to coordinate two separate billing systems (the smart card and the paper backup) rather than delivering care, especially in home health care and durables—two segments known for significant fraud. If the pilot program were redesigned for a comparative analysis between different fraud reduction approaches, one could better determine which approaches have the best return on investment.

A key lesson from modern cybersecurity research is that security technology alone will not solve a security problem unless there is effective policy implemented to control fraud. Without first plugging the policy loopholes that lead to Medicare fraud, the Federal Government will likely switch from maintaining one costly, fraud-prone system to instead maintaining two costly, fraud-prone systems.

Thank you. I am happy to answer any questions you may have.

[32] However, obtaining photos for the Medicare beneficiary demographic may prove challenging.

Mr. PITTS. That concludes the opening testimony. We will now begin questioning, and I will recognize myself 5 minutes for that purpose.

Ms. King, in 2010, the Obama administration announced that CMS would cut the Medicare improper payment rate in half by 2012, an error rate that led them to conclude $60 billion in improper payments that were made.

It is almost December of 2012. And knowing that GAO has just released a report on this demonstration project, can you tell us why the administration failed to release its mandated October report?

Ms. KING. Sir, you are referring to the Predictive Analytics Report?

Mr. PITTS. I am sorry?

Ms. KING. You are referring to the Predictive Analytics Report——

Mr. PITTS. Yes.

Ms. KING [continuing]. That was due to Congress?

I can't speak for them. I do know that it has not been submitted yet.

Mr. PITTS. Has the administration met their goal of improper payment rates being reduced by half by 2012?

Ms. KING. No, they have not.

Mr. PITTS. What did your report reveal?

Ms. KING. Well, the improper payments rate is produced by HHS. And that is not—the 2012 number was just released. And I do know that they did not meet their rate, that the rate for 2012 was 8.5 percent or $29 billion, which was slightly lower in percentage terms but higher in dollar amounts than the 2011.

Mr. PITTS. Now, Mr. Olson, in 2010, then-acting Deputy Attorney General Gary Grindler stated that, quote, "It is not enough just to prosecute and punish healthcare fraud after it occurs, we must target it before it happens through aggressive prescreening, auditing, and prevention techniques," end quote.

An all-of-the-above strategy, if you will, and while much public attention has been given to post-payment recovery efforts under this administration, do you believe that we are doing enough in aggressive prescreening and prevention techniques, and what priorities do you recommend?

Mr. OLSON. I believe that we have made a good start. But I believe that there is significant progress that needs to be made.

The prescreening methods that have been put in place are good to identify the low, medium, and high providers that are at risk. I still believe this is a beginning point and there needs to be much progress that would be made there. As well with the predictive analytics, I believe it is a starting point. I believe it is a good step that is being taken, but yet much more needs to be done, and I believe we are seeing that with the fraud prevention system that is in place. But it will continue to grow, and as the years roll on, that we will continue to see more activity in that area.

Mr. PITTS. Ms. Lavelle, you mentioned in your testimony that data sharing between public and private entities is very important for fraud prevention. Medicare Advantage seems like a good example of where public and private payers meet.

What sorts of data sharing occur between Medicare and Medicare Advantage plan companies? And do you believe that data sharing could be improved between the two to improve fraud prevention? If so, how?

Ms. LAVELLE. Mr. Chairman, I do believe there is a need to improve some of the sharing. We work through the NHCAA to share amongst all payers. And we do, as private payers, share with the government. However, oftentimes it is just a one-way street and we do not get the information back that we need. For example, if they suspend or revoke a provider, we continue to pay because we do not know who they have suspended or who they have revoked.

Oftentimes, the Department of Justice will have an ongoing criminal case and we will not be allowed to intervene with that payer during this long criminal investigation and we continue to pay bad claims.

And thirdly, there are a number of whistleblower lawsuits that involve patient harm. And until that qui tam lawsuit is unsealed, we cannot do any intervention with our providers that may be causing harm to our members.

Mr. PITTS. OK. Now, you mentioned in your testimony the Controlled Substance Utilization Monitoring Program and limiting documented prescription drug abusers to one pharmacy and one prescriber as a mechanism to prescription drug abuse and to stop the costs associated with doctor shopping.

Does Medicare Advantage or Part D plans allow insurers to implement a similar type of program? If not, do you know why?

Ms. LAVELLE. Not at this time. We have sought to get authority to do that. But at this time, they have not authorized that type of lock-in program.

And, generally speaking, our biggest problems are with the dual eligibles between the age of 20 and 40. They not necessarily are seniors. But these are the folks that have the addiction problem and are overdosing, basically.

Mr. PITTS. Thank you. My time has expired.

Chair recognize Ranking Member Mr. Pallone for 5 minutes for questions.

Mr. PALLONE. Thank you, Mr. Chairman.

I wanted to ask Ms. King initially, one of the witnesses today, I guess it was Mr. Pattinson, noted that by requiring identity verification of providers and beneficiaries, Medicare would easily eliminate more than 50 percent of the fraud within the current system.

Do you believe, you know, that that is fairly accurate or would a verification process eliminate that much of current fraud?

Ms. KING. First, I do not think we really—there is no reliable estimate of how much fraud there is in the healthcare system. So half of a total that we do not know, it is hard to say what that would be.

Secondly, I think that we just identified for the first time the types of providers that were involved in healthcare fraud. And no one, to my knowledge, has done an in-depth analysis of what the causes of fraud might be.

So I think it would be premature to say that you could eliminate 50 percent of the fraud based just on identity theft, because we do not know the extent to which identity theft contributes to healthcare fraud.

Mr. PALLONE. Let me ask Ms. Lavelle about WellPoint's anti-fraud initiatives. Does WellPoint use a smart card for beneficiaries like the one envisioned by the Medicare Common Access Card legislation?

Ms. LAVELLE. Mr. Pallone, we are on shifting sands right now with emerging technologies in the healthcare arena. We decided in the past year to pick up a predictive analytic modeling tool. And, to date, we haven't explored the smart card. We are exploring other sophisticated methods in the future, including an app that might go on a smart phone or an iPad. But we are still analyzing all the tools out there.

Mr. PALLONE. Are you aware of any of the Blues' plans that require beneficiary and provider smart cards? Do they use them?

Ms. LAVELLE. I am not aware of any that do, no.

Mr. PALLONE. As opposed to spending money on cards and card readers, where has WellPoint invested its anti-fraud dollars? If you had to pick one activity that you believe gives you the best bang for the buck, what would that be? And do you have any sense of your return on investment for these anti-fraud activities?

Ms. LAVELLE. Our most valuable tool at this time is our predictive analytic modeling tool. We are finding anomalies in systems, we are finding aberrant providers that are basically committing fraud. We are finding weaknesses in our own systems, in our own contracts, and in our own medical policies, things that we can urgently change to save dollars on an enterprise-wide basis.

Mr. PALLONE. Do you have any idea of the return on the investment, though, in terms of that?

Ms. LAVELLE. It is well over 15 to 1 at this point.

Mr. PALLONE. OK.

And then I wanted to ask Dr. Fu, I noticed in your testimony how a number of instances of fraud were committed when card readers were tampered with. Seems to me that placing multiple card readers in every physician's office just invites the opportunity for more fraud. Even an unsuspecting physician could be victimized by a faulty card reader. While that may not be happening today, isn't it conceivable that that is a danger in the future?

Mr. FU. That is a potential risk because of the software that is associated with the card readers and the connections that different components make into the clinical computing systems.

Mr. PALLONE. I am also concerned about the costs of implementing a smart-card system for all of Medicare. There is the cost of issuing the cards, the fingerprinting a million-plus physicians and new physicians, possibly the costs of getting photos of beneficiaries for the cards, and the card readers, not to mention the system changes that Medicare would need to make to accept information from this new technology.

From your experience in working in a medical setting, do you think it is reasonable to assume that each provider office would only need one card reader or do you think estimates of one card reader per office are a bit understated?

Mr. FU. I would suspect that providers would need more card readers than they originally anticipated. I say that because 17 years ago, when we rolled out a similar system in a community hospital, that was one of the areas where it was underestimated how many card readers we needed, as well as how many cards we needed to purchase, too, because the physicians and nurses would inevitably misplace the cards.

Mr. PALLONE. Let me just go back to Ms. King.

One of the things that I believe is important to keep in mind as we design our anti-fraud arsenal is that fraud is multifaceted.

Could you just take a moment to describe the different kinds of fraud that is perpetrated against the Medicare program? I know I am almost out of time, but as briefly as you can.

Ms. KING. According to the Inspector General, there are lots of different kinds of fraud, but they include billing for services that aren't needed or not provided. There are kickback schemes where people sell their numbers, sell their beneficiary numbers.

But, you know, there is a broad spectrum of fraud that is committed. But I don't think there has been a comprehensive analysis done that really drills down on all the types of fraud that have been identified. And there is, of course, a lot of fraud that goes unidentified because it is under the radar. People are committing acts that would be fraud that are not detected.

Mr. PALLONE. All right. Thanks a lot.

Thank you, Mr. Chairman.

Mr. PITTS. The Chair thanks the gentleman and recognizes Dr. Burgess for 5 minutes for questions.

Mr. BURGESS. I thank the chairman for the recognition.

Ms. King, thank very much for being here. Thank you for your testimony today.

Now, you gave us an impression in your spoken testimony that you have provided CMS a list of items that they might consider doing in order to implement the programs that they said that they are already implementing. Did I understand that correctly?

Ms. KING. Yes. We have a number of recommendations that we made to them.

Mr. BURGESS. Would it be appropriate for GAO to provide this committee with an itemized list of those things they have sent to the Centers for Medicare and Medicaid Services in order to get to the bottom of some of these inappropriate payments?

Ms. KING. We would be happy to.

Mr. BURGESS. Now, to date, has CMS replied to your provision? You have provided this information to CMS. Is it a two-way street? Are they coming back to you with the information?

Ms. KING. If we issue a report that has recommendations, the agency always has a chance to comment on them. And usually they either agree or disagree. And then we have an annual process where we follow up with them once a year to see whether they have implemented recommendations.

Mr. BURGESS. Well, that is really my question, that opportunity to agree or disagree.

In your bibliography, you referenced another report you did last month about Medicare fraud prevention, CMS has implemented a predictive analytic system.

In your recommendations part, you said HHS agreed to described action CMS was taking to address the recommendations. But my problem is, we have been talking about this for the 10 years that I have been here and we are not getting anywhere.

So how do they provide you with definitive actions that they are going—do they provide you with definitive actions that they are going to take that are associated with metrics where we could all know that they are doing what they said they were going to do?

Ms. KING. When we do our annual follow-up on recommendations, we engage in a rigorous process with them to determine whether, in fact, they have adopted recommendations.

Mr. BURGESS. When was this last annual report generated by CMS?

Ms. KING. We do our recommendation——

Mr. BURGESS. I am sorry, your——

Ms. KING. We do our recommendation follow-up each year in the fall.

Mr. BURGESS. OK. So is there a recent one that has been provided?

Ms. KING. That is an internal document to GAO. But we track that and we would be happy to provide you with a list of recommendations and the status of the follow-up.

Mr. BURGESS. That is what I was getting at. Thank you.

And, Mr. Chairman, I would like for those to be provided and made part of the record and made available to every member of the committee, because I do think that it is important.

We are all talking about the fact that we are just a few months away from Elysian Fields of the Affordable Care Act, and everyone is going to have everything that they ever wanted. But I don't know quite the number of States that have agreed to do their own exchanges, but there is a big number of States—I know my State is not going to do a State exchange—so there are a number that will fall into whatever this Federal fallback position is, which looks a lot like the public option.

And one of the concerns I had about the public option when we talked about in this committee during a markup on H.R. 3200, which was the healthcare bill that didn't become law, one of the big concerns I had with the public option was we got a lot of problem right now with inappropriate payment in Medicare. Why in the world would we expand another public program before we get our hands around this problem?

So I know the GAO does not speculate and they don't engage in conjecture. But do you have a feeling about what the future holds just a short year from now as those large public options come online?

Ms. KING. Sir, I would have to say not yet.

Mr. BURGESS. Well, I was afraid of that answer. OK.

Ms. Lavelle, let me ask you, because you are WellPoint. You are private sector. Is your company going to be developing a product that will be available in the State exchanges?

Ms. LAVELLE. I am not certain at this point. But I can find out and have someone get back with you on that.

Mr. BURGESS. Then, of course, along the same line of reasoning, you know, would you participate in a Federal exchange if there were this large Federal fallback that were provided to States that weren't going to set up their exchanges?

My understanding is this will be set up through the Office of Personnel Management, not through HHS. This is a pretty little-known and little-understood Federal agency right now that administers the Federal Employee Health Benefits Plan. But it is fixing to become an enormous Federal agency that will administer a problem—a problem—— sorry, Freudian slip—a program that is every bit as big as what CMS administers today in the Medicare system.

So I would assume a company like yours would look at that and say, this is market share, we have got to be a participant in this.

But at the same time, you have got this other problem with the medical loss ratio rules that are there in the Affordable Care Act. And I assume your company has looked at those medical loss ratios rules because they probably do affect you, do they not?

Ms. LAVELLE. Yes. Absolutely.

Mr. BURGESS. So if you spend money on fraud prevention, is that money scored as an administrative expense or a healthcare expense?

Ms. LAVELLE. We can only count the dollars up to the amount of recovery we bring in each year. So if we bring in, you know, $2 million, that is all we can count outside of the administrative costs.

Mr. BURGESS. I think you gave us a figure of ROI, of return on investment, of 15 to 1. So, presumably, that would be something you would pursue even in light of the MLR rules. Is that correct? Or is the MLR going to be an inhibitory factor for you?

Ms. LAVELLE. It continues to be inhibiting, based on our growth. We do a lot of quality of care investigations. We have found diluted chemo drugs. We have cases on cardiologists doing unnecessary stents, unnecessary bilateral cardiac caths. Maybe half of our work deals with quality of care and patient harm. And that is why we feel we should get some credit for some of the work and the prevention that we do.

Mr. BURGESS. I couldn't agree with you more.

Mr. Chairman, I would just submit, at some point, we perhaps need to have a much wider evaluation of these medical loss ratio rules and how they affect. I mean, you are talking about patients—you are not just talking about fraud, you are talking about patient safety.

Ms. LAVELLE. Exactly.

Mr. BURGESS. We just had a big hearing in Oversight Investigations on patient safety because of some altered steroids in the compounding pharmacy. Patients depend upon us to be their watchdogs on this. And the fact that you feel that this is something that is being inhibited by the Affordable Care Act, we need to get on top of that.

Now I will yield back my time.

Mr. PITTS. The Chair thanks the gentleman and now recognizes the gentlelady from Illinois, Ms. Schakowsky, for 5 minutes for questions.

Ms. SCHAKOWSKY. Thank you, Mr. Chairman.

Ms. King, I wanted to ask you a question. I think the chairman was getting at whether or not the administration has met its goals. And so the issue of how does one measure the effectiveness of fraud reduction measures. And I wanted to ask you about this.

Those that prevent fraud from happening, how would we measure that? For example, since March of 2011, CMS has deactivated 136,682 provider enrollments and revoked 12,447 enrollments, taking away their billing privileges because of, I guess, identifying them as fraudsters. And they no longer have the privilege of billing Medicare.

So how would we calculate, or can we calculate, what kind of savings are realized by this revocation of billing privileges or any other kind of prevention measure that we might take?

Ms. KING. I think there are a number of steps that CMS has taken that are in the prevention category. And one thing is strengthening provider enrollments and standards so that you are keeping out people from the get-go who shouldn't be providing services to the program.

So it is hard, you are right, it is hard to measure, well, you know, what might they have billed had they been allowed.

And I think on the other side another example is the Fraud Prevention System, the Predictive Analytic System. If you are preventing things from happening, then how do you measure the magnitude of that? And I think that is something that CMS is working on and struggling with, but it is a difficult issue.

Ms. SCHAKOWSKY. I think it is really, really important that we do that. And I think everyone on both sides of the aisle agree we need to do better. But I think it is also important that we get the metrics right so that we properly evaluate the measures that we are taking.

Let me ask you a question, Dr. Fu. As you know, the smart-card industry has legislation that would mandate CMS undertake a specific demonstration project to pilot their technology in five States.

I am not a researcher, but it would seem to me that the bill could be made better in this fashion. It seems that testing one particular intervention against doing nothing likely will yield results. But it seems to me that the better question that Medicare and Congress should be exploring is testing one technology against another technology.

So wouldn't it make more sense to test different interventions against each other to see which one is best?

Mr. FU. So in my written testimony, I have some further comments on that. I can highlight that.

I agree, it would be more telling if the experiment were comparative as opposed to absolute.

In particular, commingling the fraud reduction from the predictive analytics may make it more difficult to understand where is the reduction coming from, from the analytics or from the smart card. So it should not be conflated with the benefits from other anti-fraud mechanisms.

There are some other technologies one could try. I would say none of them are surefire. But it is a valid question to ask.

I believe one comment that was raised today was the issue of using a mobile app. And I have heard of suggestions of using an inexpensive photo ID. They all have problems. They all have benefits. But it is good to know the comparative.

Mr. PATTINSON. I would just like to add to Dr. Fu's comments that the smart-card technology is well proven around the world.

Everybody in this room probably has at least one of them on your person in the form of a SIM card in your phone. It is in the U.S. passport. The Federal Government is using them to protect all of their infrastructure.

So this is not testing a technology on the basis of does it work or not. Smart cards work in this situation for authentication and for identification. We are certainly not saying they should be done alone, and we agree that they should be done in conjunction with other technologies as they emerge. They can be included.

But at the moment, this is an easy thing to help save the Medicare system a great deal of money very quickly with proven technology, even though under H.R. 2925, we are only asking for a pilot because we want everybody to be confident that we can build the best system to save the most money to preserve the longevity of Medicare.

Ms. SCHAKOWSKY. Thank you, Mr. Chairman.

Mr. PITTS. Chair thanks the gentlelady.

Now recognizes Dr. Cassidy for 5 minutes for questions.

Mr. CASSIDY. Thank you all for being here.

Ms. Lavelle, WellPoint has MA plans. And do you have the same level of fraud, waste, and abuse in your MA plans that you administer for CMS as is reported to occur in direct fee-for-service Medicare?

Ms. LAVELLE. That is difficult to answer, Congressman.

We are very vigilant with our MA plan. We have a lot of rigorous applications, data mining programs we run against it.

One of the common denominators and one of our biggest issues is the “any willing provider” clause that allows any willing provider to bill.

Mr. CASSIDY. Are you allowed to do precertificaiton, preauthorization even if you have an “any willing provider”?

Ms. LAVELLE. On certain procedures, yes.

Mr. CASSIDY. OK. OK. So you are not sure, possibly, but just not sure.

Ms. LAVELLE. Well, I am not certain if our level of fraud in MA is the same as CMS.

Mr. CASSIDY. Got you.

Ms. LAVELLE. It is just hard to determine.

Mr. CASSIDY. OK. Now, everybody is familiar with McAllen, Texas, immortalized in the New Yorker as a place with a lot of CMS fraud, waste, or abuse. But there is a health affairs article, first author is Franzini, looking at the Blue Cross population. And in this actually McAllen, Texas, had a 7 percent lower utilization rate than El Paso.

Now, it seems like if Blue Cross is 7 percent lower in a place where—I forget the exact number—but where McAllen is like 180 percent higher than El Paso, that the problem is CMS, frankly. And the authors of the paper at the end postulate what could be the problem. Some of them are reflected in your GAO report.

Would you like to render an opinion on that?

Ms. LAVELLE. I am not familiar with the article, so I’d rather not.

Mr. CASSIDY. What would be your estimate of why Blue Cross Texas has 7 percent lower expenditures in McAllen, whereas CMS has, again, I wish I had looked at—80 percent or 180 percent higher than the cohort city, if you will, the comparison city?

Ms. LAVELLE. I think we do have some sophisticated tools in place that stop the dollars before they go out the door.

Mr. CASSIDY. So that suggests that CMS does not.

Ms. LAVELLE. No. I am not suggesting they do not. But we are very competitive in the Blues. And we are very collaborative between States in warning each other, giving early warning signals. But we do have very rigorous special investigation——

Mr. CASSIDY. Got you. The only reason I am cutting you off is time is limited. And it does seem as if the Blues have something that CMS does not, which is a little daunting when we figure we are turning over our healthcare system to them.

You mention in your testimony, I think it was you, about the duel eligibles being able to change Part D plans month to month. And so those seeking drugs will try and stay one step ahead.

Ms. LAVELLE. Yes.

Mr. CASSIDY. Do you have an estimate of how much money we would save? Because prescription drug abuse is a huge problem.

Ms. LAVELLE. It is.

Mr. CASSIDY. Do you have an estimate of how much we would save were we to limit that activity?

Ms. LAVELLE. I don't have an estimate. But I can tell you that a single provider that we lock into place with a single ER for non-emergency use, we could save at least 300,000 to 400,000 a year based on——

Mr. CASSIDY. Three hundred, four hundred thousand what?

Ms. LAVELLE. Dollars a year, per member.

Mr. CASSIDY. Per member.

Ms. LAVELLE. For locking them in. They evade the lock-ins by jumping from WellPoint to Humana to Aetna.

Mr. CASSIDY. You would save $300,000 per member, per year?

Ms. LAVELLE. For every dollar we spend on drugs, we have determined that we spend approximately $41 on facility fees.

Mr. CASSIDY. And any clue the size of this population that you would save $300,000 per year on? I mean, is it a thousand people? Is it a million people?

Ms. LAVELLE. It is hard to say. But it is——

Mr. CASSIDY. Ballpark.

Ms. LAVELLE. We probably have a thousand right now that we are monitoring. And we just don't have the manpower to monitor——

Mr. CASSIDY. So a thousand times 300. We are talking about real change here——

Ms. LAVELLE. Yes.

Mr. CASSIDY [continuing]. For one company. Granted, a big one.

Ms. LAVELLE. Right.

Mr. CASSIDY. Dr. Fu, I really liked your testimony, man. I will tell you, the TWIC card was supposedly going to be the answer for all security problems, and I get regular complaints from people fighting about the TWIC card. And I like the way you kind of, if you will, puncture a couple holes in its foolproofness.

Is there anything short of a retinal scan that could actually make a secure ID card? Because you mentioned, if somebody gives their card to somebody else and they can take that number, et cetera, et cetera.

Mr. FU. Thank you, sir.

Identity is very difficult to establish. In computer security, there are three basic ways to do it. You can use something you have, like a smart card; something you know, like a password; or something you are, like a fingerprint. Whereas we also like to call it something you lost, something you can't remember, and something you were.

But I would say that the difficulty is in how the smart-card system is used in the greater system. So it doesn't matter if you have the most secure technology or even if there is a flaw, if that system is put as a component in a larger system that it itself has flaws. For instance, a paper-based——

Mr. CASSIDY. Got you.

Mr. FU [continuing]. Alternative system would leave that door open to fraud.

Mr. CASSIDY. But still within that, there has to be—and you point that out—there has to be things about the card itself even in a perfect system that can make that system vulnerable.

So I go back to again is anything besides the fingerprint or a retinal scan going to give you the assurance that somebody sitting at a computer terminal is just not filing claims for things not done?

Mr. FU. Unfortunately, despite decades of research in computer security, there is no silver bullet. There is no surefire way to establish identity. I think one of the reasons that certain identity cards work well in buildings is that you may have police nearby or people watching or people who would catch you.

So I don't have a good answer for you on what would work better. I do think it is a good idea to try different alternatives because different contexts you will see different technologies having different advantages.

Mr. CASSIDY. Thank you, Mr. Chairman. I apologize for going over.

Mr. PITTS. Thank you. The Chair thanks the gentleman.

The Chair recognizes the gentleman from New York, Mr. Engel, for 5 minutes for questions.

Mr. ENGEL. Thank you very much, Mr. Chairman.

Mr. Saccoccio, in your testimony, one of your recommendations is that we ensure a skilled and sufficient workforce of anti-fraud professionals. My sense is that no matter how much we invest in front-end screening or technology solutions, we will still have a need for those boots on the ground.

There are providers who look legitimate on paper and it is only until an unannounced visit that we discover something is wrong. Sometimes it is not until a beneficiary is interviewed or calls to report something suspicious that investigators get a hint of problems.

So my question is, can you talk about what kind of anti-fraud workforce CMS should maintain? Do you believe additional investments in anti-fraud funding, including for personnel, would be valuable to help fight Medicare fraud?

Mr. SACCOCCIO. Yes. Thank you for the question.

I definitely agree that technology is not the silver bullet. It is a tool that has to be used. Predictive analytics is important. It is going to give you a lot of leads. But once you get those leads from the technology, you need the people to examine those leads.

I don't know of any system right now where you could just flip a switch and based on the information you get back from a computer be able to automatically deny a claim or suspend a claim until there is some sort of investigation done.

So you definitely need folks that are very savvy with technology, experts in technology. You need folks able to analyze data that is generated, statisticians, those types of folks. You need folks that have clinical backgrounds, because as a few of the witnesses talked about, a lot of the issues involve quality of care, necessary care. So you need folks that have clinical backgrounds.

And then you need investigators, folks that know how to do investigations, folks that can go out into the field and ask questions and visit sites where potentially you have phantom providers or fraudulent providers.

So you need a mix of workforce. So definitely any resources that are put into this, some have to be focused on technology. But you also have to ensure that you have the right type of workforce to go out there and conduct the investigations and validate the information that the technology is feeding you.

Mr. ENGEL. Thank you.

Let me ask you again, Mr. Saccoccio, and also Ms. King, the Affordable Care Act contains a number of provisions designed to promote data sharing between agencies, the Federal Government, and the States, and also various Federal healthcare programs. And it also, as you know, provides new tools and strengthens penalties against fraudulent providers.

The CBO, the Congressional Budget Office, estimates that these anti-fraud provisions when fully implemented will save American taxpayers $7 billion over the next 10 years.

So let me ask you again, Mr. Saccoccio, and also Ms. King, what specific aspects of fraud detection do you think are being most positively impacted by the provisions in the Affordable Care Act and what additional steps do you believe Congress should take to enable better fraud detection and prevention?

Ms. King, why don't we start with you.

Ms. KING. Yes. Well, one of the key provisions of the Affordable Care Act was a set of provisions strengthening the ability of CMS to screen providers before they are enrolled in the program. So you are ensured that you are only getting legitimate providers in the program.

And as part of that process, CMS also contracted with a couple of contractors to do onsite inspections to go up, you know, for high-risk providers to make sure that they are, in fact, legitimate businesses and to automate the enrollment process more quickly so that you can see before you enroll someone whether they are on the do-not-pay or the excluded list.

So those kinds of things I think have a good bit of potential.

Mr. ENGEL. Thank you.

Mr. Saccoccio?

Mr. SACCOCCIO. Yes. I think the biggest thing in the Affordable Care Act, as Ms. King mentioned, is the ability, giving CMS greater ability to screen providers coming into the program.

And I think some of that is going to require, depending on how you establish—when you look at different providers, you have to establish potential risks from those different types of providers. So the greater risks that you anticipate, the more screening you will have to do, which may require some onsite visits for things like DME companies, to ensure that these are actually valid companies that are actually in business.

But I think one of the steps looking to the future is that a lot of this information that is coming out of their automated screening process that CMS is doing has to also be incorporated into their Fraud Prevention System.

In other words, connecting the dots, not—as you screen providers, to make the network connections between different types of providers. Because what you have is are often put up as fronts for different companies. And as you establish who these folks are, you'll see that there are connections with other folks that are actually committing fraud.

So I think a big piece of that is doing the screening, but then incorporating what you are finding out from that screening and what you are also doing with respect to claims analysis and predictive analytics.

Mr. ENGEL. Thank you.

Thank you, Mr. Chairman.

Mr. PITTS. The Chair thanks the gentleman and now recognizes the gentleman from Georgia, Dr. Gingrey, 5 minutes for questions.

Mr. GINGREY. Mr. Chairman, thank you.

And I want to thank all of the panelists, all of the witnesses. I am going to direct my questions primarily to the member from the Government Accountability Office, Kathy King. So, Ms. King, it will be primarily directed toward you.

I will kind of follow up on what my colleague from New York, Mr. Engel, was just referencing regarding the provisions in the Patient Protection Affordable Care Act, Obamacare, toward combating waste, fraud, and abuse. And I think he gave the figure of an estimated savings of $7 billion over 10 years if these provisions of Obamacare were implemented.

Ms. Lavelle testified that WellPoint's anti-fraud activities rely in part on a system of identifying high-risk practices, providers, and beneficiaries, and then creating solutions such as prior review to deal with these problems.

The Patient Protection and Affordable Care Act created a number of—in fact, I think at least eight anti-fraud provisions, such as granting the Secretary the authority to conduct criminal background checks for providers and suppliers considered high risk.

Ms. King, you referenced that.

Can you tell me whether this administration has, to date, implemented all of these provisions that are in the law in Obamacare?

Ms. KING. I cannot, because our process of checking on them is not complete. But, you know, in the spring when we also testified about this issue, there were a few provisions, including the criminal background check and surety bond provisions, that were not yet implemented.

Mr. GINGREY. Let me help you a little bit. You say you cannot answer the question on what has been implemented.

Section 6407 of Obamacare created a requirement that CMS implement face-to-face encounters between patients and providers before a physician can certify eligibility for durable medical equipment.

While the State of Georgia has many good and hopefully honest and mostly honest DME providers, we all know that durable medical equipment is one of the most fraudulent areas in Medicare and has garnered nationwide scrutiny on programs even like "60 Minutes."

Can you tell me, has the administration implemented face-to-face provider meetings for DME to date? Have we done that?

Ms. KING. Not to my knowledge, they have not. Ordinarily, if I were appearing before a committee, I would check on all of those things, but I did not have the opportunity to fully check all those things before coming today.

Mr. GINGREY. Well, look, I am going to help you again. And I said there were eight things I think you—maybe CMS has implemented one of the eight. But let me list, just read to you a number that have it, including this face-to-face encounter in regard to prescribing durable medical equipment.

Implement checks to make sure that a physician actually referred a Medicare beneficiary for medical service—for example, clinical laboratory—before paying the claim.

No, they have not done that.

Implement a surety bond on home health agencies and certain other providers of services and supplies.

No, they have not done that.

Establish a compliance program for fee-for-service providers and suppliers.

Once again, no, that has not been done.

Implement a temporary moratorium for new Medicare providers from enrolling and billing the Medicare program even though there are more than enough suppliers to furnish healthcare services in certain areas of the country.

No, they have not done that.

Mr. Chairman, I believe this committee should find out what powers CMS has. Many of them, as Ms. King indicated, and others, that were granted in the law which is now over 2 years old to help implement waste, fraud, and abuse that it currently does not employ. So how are we going to save that $7 billion over the next 10 years.

My opposition to Obamacare in this committee certainly is well known. I do believe that protecting taxpayer dollars and Medicare dollars from fraud and abuse is one of the main charges of this government and that we as committee members have.

And it is very much a bipartisan issue. Medicare is set to go bankrupt as early as 2017, as late as 2024. If this administration has the authority to implement changes within the Medicare program that could prevent billions in lost funds annually and it is not using them, I believe, Mr. Chairman, that the administration owes us an accounting of the reasons why to date, 2 years, seven out of eight provisions have not been implemented.

And I yield back.

Mr. PATTINSON. Mr. Chairman, Congressman, I would like to make a comment.

Mr. PITTS. Go ahead. You may.

Mr. PATTINSON. I think you are describing a very significant problem about the DME issue of being able to deliver equipment and have it prescribed without physical contact.

Looking at the pilot that we once proposed under this Medicare CAC Act, I would suggest that that is exactly a very good reason why we could use the twin card approach; a provider and a patient must both combine their cards in a reader to perform the transaction to show that they have authorized this particular DME equipment for this provider, by this provider for this individual. Then subsequently on delivery. Then we know who was responsible for issuing that request.

So no nefarious claims or no nefarious deliveries of DME equipment can now take part on the basis that you have to have two keys to make that request work. So I would strongly recommend that we include that as part of the pilot.

Mr. PITTS. All right. Thank you.

The Chair now recognize the gentleman from Illinois, Mr. Shimkus, for 5 minutes for questions.

Mr. SHIMKUS. Thank you, Mr. Chairman.

Apologize for not being here for all the opening statements. Thanks for your testimony. In this era of budget crises and entitlement reform, to think that we wouldn't do some simple steps to get a handle on waste, fraud, and abuse is unbelievable. Frustrating from those of us.

Mr. Pattison, just for a second, and you mentioned it earlier in one of the questions, H.R. 2925, which I am a co-sponsor of, bipartisan support, is what type of a program?

What is the intent of 2925?

Mr. PATTINSON. It is to operate a pilot——

Mr. SHIMKUS. A pilot program.

Mr. PATTINSON. Pilot program of five regions.

Mr. SHIMKUS. How are the region to be chosen?

Mr. PATTINSON. The regions would be defined the by agency implementing the——

Mr. SHIMKUS. And it is my understanding under the highly abused areas of——

Mr. PATTINSON. If that's what they so choose, that would be where they would have the best effect.

Mr. SHIMKUS. That is the intent.

Mr. PATTINSON. Indeed.

Mr. SHIMKUS. I think that is our intent.

Mr. PATTINSON. The pilot would be to upgrade the Medicare cards for the beneficiaries by taking the number off the card and providing the card, such as the one I have in my hand here. It would also be providing a similar smart card, but with more capability to the provider. Then by using the terminals at the various locations, which, by the way, with a Chip and PIN implementation coming out, these terminals are going to become prevalent all over the place, anyway. So we are just adding basically functionality to existing terminals that will exist by the time we get around to a pilot.

But by putting the two cards in the same unit, performing the PIN actions of the beneficiary and the fingerprint of the provider, we conceal those transactions and prevent people from creating transactions without any of these technologies.

So think of it like a safety deposit box in the bank; you need to have two keys to make this drawer open. You need to have these two keys to make these transactions work.

So the pilot is to test this. And to date Dr. Fu's testimony, it is to make sure we design the very best and most robust system for a potential rollout.

Mr. SHIMKUS. And, Mr. Terzich, do you want to add to this discussion on the use of the card?

Mr. TERZICH. Mr. Congressman, I would add the following. Essentially, when you look at, both from the government and from the private sector perspective, the pervasive deployment expansion of smart cards and smart chips, you know, today there are literally billions of smart chips in circulation, millions of smart cards in circulation. And despite some random rogue instances of security breach, the underlying technology has demonstrated time and time again that it is a very productive, useful technology.

And when you apply that to the challenge at hand here where there is a very optimal opportunity to engage in the low-hanging fruit by simply deploying some technology, that I think would in many respects take a big slice out of the abuse and the fraud that exist today.

Mr. SHIMKUS. I have no understanding why we would not move immediately to do this as a start. Not the entire solution of waste, fraud, and abuse in the system. But this is really a no-brainer. Twenty million Department of Defense individuals use this system. This is not—this is not new technology or new activity that no one has used before.

So the other thing I would like to add on is, Mr. Pattinson, how about international—well, let me start by this too, because my frustration is pretty high on our challenges that we face in this country.

If anyone uses their credit card overseas today, theft comes by someone stealing your slip, not through the technology.

If anyone uses a passport, these new passports that we have that swipe through the system, they are using this with biometric facial identification. I mean, folks, we are using this now. All we are asking is that let's try it to highlight waste, fraud, and abuse.

I want to move to Ms. Lavelle real quick.

Your testimony is also illustrative of an issue with the healthcare law, fee for service, and Medicare Advantage. And I would hope that when you go back, you would ask to do an analysis of the waste, fraud, and abuse under fee for service versus waste fraud and abuse in dollars. You have to get some statistician that would make it equal sizes or whatever they have to do to make sure.

But I would wager money that fee for service is multiple times more abusive in waste, fraud, and abuse. And the argument I would postulate is that you have an organization established and folks making sure that there is not waste, fraud, and abuse going out the door, and that is that whole medical loss ratio debate and what is going to be able to be paid for.

So if we don't allow companies to do their due diligence because we don't let them qualify in the medical loss ratio, guess what, we are going to have more waste, fraud, and abuse. It is the most ludicrous thing that I have seen. We need market, we need competition. The private sector does that because they don't want to lose the money.

With that, Mr. Chairman, I think we need to have many more hearings on this issue.

Thank you all.

Mr. PITTS. The Chair thanks the gentleman and now recognizes the gentlelady from Tennessee, Ms. Blackburn, for 5 minutes for questions.

Ms. BLACKBURN. Thank you, Mr. Chairman.

And I want to thank each of you for your patience, sitting through this hearing, being here with us today.

Ms. King, thank you for your report. I appreciate that you got that in to us in a timely manner, and I appreciate the way that you broke it out, looking at medical facilities, durable goods, and where the problem exists.

I think for those of us that have been focusing on this waste, fraud, abuse issue in the Medicare/Medicaid systems, and this is not a new problem, what we have come to realize is that HHS as a whole doesn't put enough attention on this issue, and that we still have a broken system, and that the pay and chase model does not yield the results that we need.

And I can tell by looking at your nodding heads you all agree with that.

I will say this. I am disappointed that we did not get the Medicare report that was due to be made public on October 1 looking at these issues. And my hope is that we are going to see this soon.

I do want to ask you, Ms. King, did you all look at the contract that was given to Northrop Grumman in 2011 to develop a system? We had the bureaucrats there at Centers for Medicare and Medicaid at CMS that gave a $77 million contract to have Northrop Grumman in 2011 to come up with a fraud prevention system. Did you all look at this contract and the miserable yield that has come from that with its first eight months of implementation?

Ms. KING. We evaluated the implementation of the program. But we did not look specifically at the contract.

Ms. BLACKBURN. OK. But I think you can say if we spent $77 million in 8 months into the implementation, we have seen a $7,591 return from that investment, that it is pretty poor, pretty poor investment.

I want to turn to Mr. Saccoccio, Mr. Terzich, and ask you all, if you were given a $77 million contract, how would you go about—what would your advice to Medicare, to CMS be on solving this problem? Would you have a ready answer? Would you have a way to move forward to help CMS, to help companies like WellPoint in identifying this fraud before it is committed?

Mr. SACCOCCIO. You know, the CMS contract and their implementation of this Fraud Prevention System, from our viewpoint, it is definitely a road they have to go down. Now, whether or not, you know, the cost of that contract and who they decided to go with, with respect to that contract, I have no particular information on that. But definitely predictive analytics and predictive modeling, those are the things that they have to be doing going down the road.

Now, sometimes I think what happens with these systems is that, with respect to suspension of payments, I know they haven't started where they are actually suspending payments based on the——

Ms. BLACKBURN. Well, in the interest of time, let me interrupt you now.

Do you know private sector companies that could probably solve this and solve this problem quickly?

Mr. SACCOCCIO. It is hard to say. I know some of the health plans are using predictive modeling of some sort. About 40 percent of our members do. And as Ms. Lavelle mentioned, they are having success with that.

So I think, you know, obviously, the implementation, there are more efficient ways of doing things. But not being part of that process, it is very hard for me to say.

Mr. TERZICH. Congresswoman, can I add a comment here?

Ms. BLACKBURN. Yes, you may.

Mr. TERZICH. You know, when you have look at the challenge that we face, I think it is the sum of a variety of technology-based solutions that can make a big impact.

And beyond predictive analytics, you know, you have the opportunity in H.R. 2925 to add the electronic handshake that occurs. And that information that gets processed in real time, in combination with predictive analytics, is going to increase visibility throughout the process.

And from our private commercial experience in business, what you see is the more visibility you apply to the process through the use of technology, the more opportunity you have to refine those processes over time. And so it is much more of a journey than an event. But it creates a tremendous opportunity.

Ms. BLACKBURN. So what you are saying basically is, with the existing technologies and with the existing platforms that you all have created in the private sector, we could create a pathway that would place the necessary firewalls and the necessary handshakes and the necessary screenings and prequalifications that would eliminate much of the fraud, which has now become big business in Medicare/Medicaid, so big that we have even had the Secretary of HHS before us say they don't know exactly how big it is, if it is a $4 billion a year or $10 billion or $100 billion.

The issue is, we have to find a way to track it and eliminate it and prevent it from occurring because pay and chase doesn't work. So what you are saying is you all have the items that are necessary.

I yield back, Mr. Chairman.

Mr. PITTS. The Chair thanks the gentlelady.

I ask unanimous consent that Congresswoman Christensen and Congressman McKinley be allowed to address our witnesses for 5 minutes.

Without objection, so ordered.

Dr. Christensen, you are recognized for 5 minutes for questions.

Mrs. CHRISTENSEN. Thank you, Mr. Chairman. And, again, thank you and thank the ranking member for allowing me to sit in on this hearing.

And thank the panelists for being here.

Mr. Saccoccio, one of the points you raised in your testimony is that information-sharing—and others did, too—and cooperation among all players of health care is critical. And you spoke about collaboration between HHS, I guess, and DOJ.

But could you talk a little about the current information-sharing that might be taking place between private and public sector and what more could be done? And any specific examples you might have of how that public-private partnership and sharing of information has led to some success in cracking down on fraud?

Mr. SACCOCCIO. Yes, as I mentioned in my testimony, information-sharing is critical between the public and private sides. You have a healthcare system where you have multiple, multiple payers. None of them get a complete view of everything that is happening out there. Therefore, it is incredibly important that they share information.

Some of the things that are happening right now, my organization, NHCAA, our members consist of health plans, about 90 health insurers, but we also partner with the public side, as well. So the CMS, the IG's office at HHS, the FBI, they all participate with us. And the things that we do, we actually have meetings where everyone sits around a table and talks about what they are seeing, what the emerging schemes are, what the emerging trends are, so that you could take that information back and look at your own data and your own plan. So that is happening.

We have a database of investigations so that if a private insurer, say, WellPoint, opens an investigation and puts that information into the database, that information is available not only to other health plans but also to law enforcement, FBI. So that kind of information is being shared.

We also have a process by which if there is an open investigation that, say, the FBI is conducting and they want to know whether there was any private exposure on the private side for private health plans, they can query us, and we go out to the private side members to see what kind of exposure there may be.

So those types of things are happening.

What I see with this Health Care Fraud Prevention Partnership, I think that allows us to potentially take it to the next level, where you could actually have data exchanges, data analysis done, where private health plans could take a look at their data, the government could take a look at their data, say, in Medicare fee for service and Medicaid, and on particular topics come together and share that data to see what each payer is seeing so that you can anticipate that.

A good example of this was, back in 2010, we had an information-sharing meeting at NHCAA that we hosted in Florida, where we had the FBI, the inspector general's office at HHS, local law enforcement, private payers, all came together to discussion the infusion therapy fraud in south Florida. And based on that, the private insurers found out that they had about a half a billion dollars of exposure from infusion therapy fraud just based on the information that they were able to obtain from CMS and vice versa.

So it is incredibly important in the environment that we have that, as information comes out from the various data analytics that different companies use and that CMS may be using, that as they see different things, that they share those with the other payers so that they can go back and see what kind of exposure they may have.

Mrs. CHRISTENSEN. Thank you.

Dr. Fu, we had at least two testimonies about smart cards, and we can see that they would provide protection. But one of the problems that was noticed in a National Health Law Program fact sheet was that they can also be a barrier to access and perhaps, this article suggested, that identity verification programs reduce costs by discouraging eligible beneficiaries from obtaining the cards and, therefore, the benefits, rather than from preventing fraud.

So my question to you is, do you think in these pilot programs this is another factor that should be included in assessing——

Mr. FU. I do think a pilot program should look at both—or not only the benefits, but also the risks, including the clinical care and potential patients who may not receive the care they would have otherwise had.

Mrs. CHRISTENSEN. Thank you. And——

Mr. PATTINSON. If I could comment, the fact that they have the card or not today, in terms of their care, it shouldn't detract in any way or make it any different to what we would have if we did a smart card implementation. The patient should always be getting their care and not have any negative effect.

So I don't see any difference between what we do today as well as what we could do with a smart card. You are not going to get denied service. We are just trying here to stop the fraud.

Mrs. CHRISTENSEN. It is just the hurdles that they have to go through to get the card. And for a person that might be disabled, poor, poorly educated, there are barriers there for them to really access the card and, therefore, the benefits.

Mr. PATTINSON. I am sure you have a good point, Congresswoman. The fact that the ATM cards and everything, they are using bank cards today, debit cards, credit cards—this is nothing more than a card and a PIN. And, yes, there will be instances where PINs are hard for those to manage, and in that case we need to have the right policy and the right part of the pilot to work out how to correct those situations.

Mrs. CHRISTENSEN. That was the point of my question, that it should be a part of the pilot so that we could make sure that, while they provide the security, they don't increase the barriers. Thank you.

Thank you, Mr. Chairman.

Mr. PITTS. The Chair thanks the gentlelady.

That concludes round one. We will go to one follow-up per side.

Dr. Burgess, you are recognized for 5 minutes for a follow-up.

Mr. BURGESS. I thank the chairman for the recognition.

Ms. King, let me just ask you. You guys have done some extensive study on the fraud prevention system at CMS, and you have prepared a report. Can you give us an idea of what is the number of fraudulent claims that have been stopped dead in their tracks by this fraud-prevention system?

Ms. KING. Not exactly. I can't, sir. But, you know——

Mr. BURGESS. Well, let me ask you this: Has there been one instance where a claimed dollar didn't go out the door because of this fraud-prevention system?

Ms. KING. I don't believe that they are stopping payments yet. And I think the way the system was designed, it was not intended to be an automatic stopping of payments in most cases. The way it is designed is that it flags problematic claims and problematic payments so that then those things are investigated to determine whether they appear to be fraudulent.

Mr. BURGESS. Your answer is not giving me—I mean, I talked about the Elysian Fields and the problems that are ahead. You are not giving me a great deal of confidence that the dollars aren't going to fly out the door at an even faster rate and end up in places where they shouldn't be.

Now, one of the things I have talked about before and I mentioned in my opening statement, do you think there are a sufficient number of Federal prosecutors to be able to bring the prosecutorial case for fraud when it is discovered?

Ms. KING. We are currently in the process of evaluating the use of the healthcare control account which provides funds to DOJ, the FBI, and the OIG. So we will be in a better position to evaluate that later this year.

Mr. BURGESS. And once again, you are not giving me a great deal of confidence here.

You know, when I send one of my staff members with my personal credit card down to Chick-fil-A to buy lunch for the office, I get a call back that says, Hey, your card is being used to charge $100 worth of Chick-fil-A here; is that OK with you? Why can't it work that way in the CMS world?

Ms. KING. You mean that there is an automatic response?

Mr. BURGESS. Yes. When something appears out of the ordinary. "This isn't something that we normally see in the conduct of your business day, Doctor. Here is some evidence that may be of interest to you." And I say, "No, no, it is fine. You let them go ahead and have the Chick-fil-A." But why is it so hard in your world, or CMS's world I should say, for that to happen?

Ms. KING. I don't know the exact magnitude of the cost, but I think implementing something like that—and I have gotten phone calls, too, from the grocery store before I have gotten home, "Did you charge this?" I think that technology is expensive.

Mr. BURGESS. Apparently it is worthwhile for Visa. Because what is their fraud rate? .03 percent? And CMS's fraud rate is anybody's guess, but 10 percent or whatever it is?

Ms. KING. You know, we have not been able to determine what the fraud rate is in——

Mr. BURGESS. I get you.

Ms. KING [continuing]. Government or private health plans.

Mr. BURGESS. But I would suspect that WellPoint is not in the business of letting all of their dollars go out the door inappropriately.

Is that correct, Ms. Lavelle?

Ms. LAVELLE. Yes, that is correct.

We have two prepayment review programs going, one in New York, one out of Chicago. Just last year alone, in placing some of these providers on prepay review where we turn off their ability to file electronically, they send in medical records, we have saved $18 million, just in the New York market. So that is one of our most aggressive and useful tools right now.

Mr. BURGESS. Yes. As a provider, I would hate that. But at the same time, when you are dealing with the problem, the magnitude that we are seeing, and you are fixing to expand it—you know, let's be honest. The Affordable Care Act, the States that aren't going to do a State exchange, that are going to do the Federal fallback, I mean, this creates an entire new dimension for fraud, which brings up the other point.

How at WellPoint are you staying ahead—you know, some of the stuff we heard on Homeland Security, you have to learn to think like a terrorist. How are you learning to think like a criminal who wants to defraud the healthcare system?

Ms. LAVELLE. Well, we try to stay ahead with the emerging technologies. We are looking at devices, pharmaceuticals, procedures. Every week there is something new that comes out.

The providers have consultants which tell them how to bill for these things. Even though they are investigational and not covered, they get counsel on how to bill for them under conventional coding. So we are constantly looking at those devices and trying to stop a lot of them on the dime.

The providers actually advertise the new devices on their Web site and tout that they are covered by most insurers. And we have shut several of them down in the last few years.

Mr. BURGESS. But to reemphasize the point, those dollars spent on that activity would be scored as administrative dollars——

Ms. LAVELLE. Exactly.

Mr. BURGESS [continuing]. Under the medical loss ratio. In fact, you are not going to be rewarded for doing that in the new system under the Affordable Care Act. You will be penalized to some degree for your fraud-prevention activities.

So in an odd way the Affordable Care Act is creating new opportunities for fraud and penalizing you if you decide that you are not going to pay these dollars out inappropriately. It is a recipe for fiscal disaster.

Thank you, Mr. Chairman. I will yield back my time.

Mr. PITTS. The Chair thanks the gentleman and now recognizes the ranking member, Mr. Pallone, for 5 minutes for follow-up questions.

Mr. PALLONE. Thank you, Mr. Chairman.

I had one question, but I wanted to clarify the record. When Dr. Gingrey mentioned that CMS had not implemented the face-to-face requirement from the Affordable Care Act, that is not correct. The face-to-face requirement for durable medical equipment was implemented in this year's physician fee schedule rule, and home health face-to-face requirements were implemented in 2011.

The other thing, I wanted to respond to Ms. Lavelle's testimony and Mr. Shimkus's stating that the medical loss ratio formula undermines fraud-fighting activities by insurers. In fact, the medical loss ratio requirement in the ACA is a critical consumer protection that has already saved consumers over a billion dollars. HHS followed the NAIC position on how to characterize the fraud-fighting activities and provided some room for insurers in the formula.

And fraud-fighting is an administrative activity, and I don't think it should become an open-ended loophole to undermine the medical loss ratio. The formula fairly allows some moneys to be deducted from the administrative side of the formula but balances that against undermining this important consumer protection, in my opinion.

I wanted to ask Dr. Fu, I have this article that discusses students at Cambridge University in England, and it finds—basically what they did is they crashed the chip and PIN system. Have you seen this before?

Mr. FU. I am not familiar with that particular article, but I am familiar with the work.

Mr. PALLONE. Yes. So, I mean, if this is happening with the secure card now, isn't there a danger of that in Medicare? I mean, how do we—you know, I know it is Cambridge and they are smart, but isn't there the same risk?

Mr. FU. Well, I think these—you cannot underplay the risks. There will inevitably be problems in any technology. But one thing for sure, it is not a silver bullet. And, in particular, there can be some vulnerabilities in the software associated with interfacing with readers.

Mr. PALLONE. And, Mr. Pattinson, since I brought this up, I should give you an opportunity to comment on that, too, if you want. I noticed the British accent, so maybe you are familiar with Cambridge and what is going on there.

Mr. PATTINSON. Well, I am an American citizen, Congressman, but, yes, that is my roots.

I would say that in all these instances that you find it is not the card technology that has been compromised, it is the system that it has been involved in. And with the good offices of good security professionals like Dr. Fu, we often engage these people at Cambridge ourselves and hire them to actually try and attack our systems. And on that basis we can make better improvements for the future rollouts.

So for any Medicare pilot and potential rollout, we would ensure that we have all of the lessons learned from these other situations where the systems have become and are identified as vulnerable and make sure that we implement the technology which is the best for this Medicare program and, therefore, the best for sustaining the longevity of this benefit program.

Mr. PALLONE. All right. Thank you very much.

Thank you, Mr. Chairman. I yield back.

Mr. PITTS. The Chair thanks the gentleman.

That concludes the testimony. If Members have questions for the witnesses, I ask that the witnesses respond to the questions promptly. I remind Members that they have 10 business days to submit questions for the record. Members should submit their questions by the close of business on Wednesday, December the 12th.

Mr. PITTS. Excellent hearing. Thank you very much for your testimony.

Without objection, the subcommittee is adjourned.

[Whereupon, at 12:12 p.m., the subcommittee was adjourned.]

[Material submitted for inclusion in the record follows:]

**Opening Statement**
**Chairman Fred Upton**
**Energy and Commerce Subcommittee on Healtb**
**"Examining Options to Combat Health Care Waste, Fraud, and Abuse"**
**November 28, 2012**

Medicare faces considerable challenges that will need to be quickly addressed to preserve the program for future generations.

On the current fiscal trajectory, the Medicare program will likely be bankrupt by 2024. However, according to one scenario outlined by the Medicare Actuary, insolvency could happen as early as 2017 – less than five years from now. The Congressional Research Service has determined that if the program does go bankrupt, Medicare will be unable to pay seniors' health care bills absent legislative action. Major reform of the program is needed to rescue it from bankruptcy and preserve access to health care for America's seniors. In addition to reforming the system, our federal government must get better at safeguarding taxpayer dollars and ensuring that spending in Medicare is only for services that improve the health and well-being of Medicare beneficiaries.

Among the greatest threats to Medicare is the enormous amount of money that the program loses to waste, fraud, and abuse. Although the true annual cost of fraud and abuse in health care is not known, the Centers for Medicare and Medicaid Services (CMS) estimated that in fiscal year 2010 these two programs made more than $65 billion in "improper federal payments," defined as payments that should not have been made or were made in an incorrect amount.

CMS' estimate of improper payments is likely to understate the true extent of the problem. For example, an April 2012 study by former CMS administrator Donald Berwick and RAND Corporation analyst Andrew Hackbarth estimated that fraud and abuse added as much as $98 billion to Medicare and Medicaid spending in 2011 and a study from the Institute of

Medicine estimates health care fraud at $75 billion a year and found that about 30 percent of health spending in 2009 -roughly $750 billion - was wasted on unnecessary services, excessive administrative costs, fraud, and other problems.

The federal government has stepped up its efforts to identify and prosecute fraudulent schemes, but much more needs to be done. Specifically, we need to be more proactive in implementing tools that prevent improper payments from happening in the first place.

Our witnesses were invited to testify to the methods currently employed by CMS as well as emerging technologies used in the private sector that might improve the integrity of the Medicare program. We appreciate their time and expertise.

**Opening Statement of the Honorable Cathy McMorris Rodgers**
**Subcommittee on Health**
**Hearing on Examining Options to Combat Health Care Waste, Fraud and Abuse**
**November 28, 2012**

*(As Prepared for Delivery)*

Earlier this year, the Medicare Trustees report made some grim predictions. The trustees calculated the Hospital Insurance Trust Fund (Part A of Medicare) would be able to stay solvent only until 2024. They warned that action is needed to secure its long term future.

With 48.3 million people covered by Medicare in 2011 and 10,000 baby boomers added each day to that number, we must have serious discussions about how to keep Medicare solvent for future beneficiaries.

Identifying true fraud and waste in Medicare is one part of the discussion.

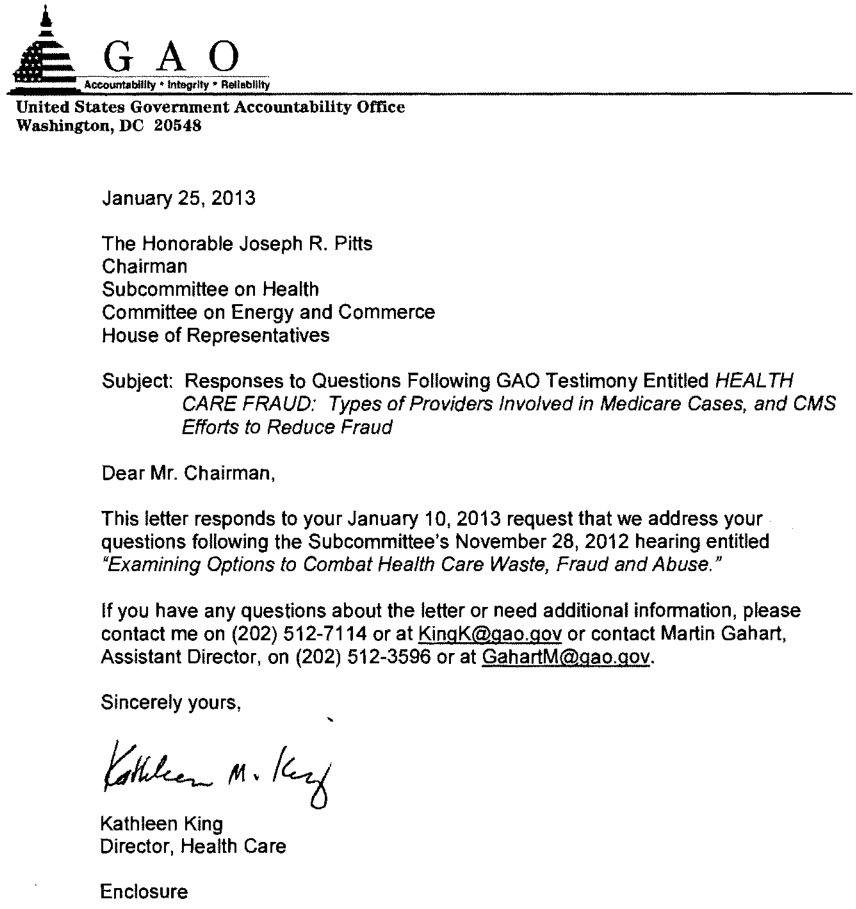
Today we learned that CMS implemented its Fraud Prevention System in July of 2011.

This system uses predictive analytics to identify potentially fraudulent claims in a prospective manner. This is an important first step in moving away from chasing true fraud to preventing fraud. However, this system needs further work, including the identification of appropriate performance goals.

We have also learned of "smart card" technology that would, among other things, remove a beneficiary's social security from their Medicare card. CMS has been asked to identify ways to do this and I think this should be a priority to protect the identity of seniors.

As we move forward in this discussion of fraud and waste in Medicare, I think that it is important to remember that most Medicare providers are honest people trying to provide quality medical care to their patients. We should seek input from these providers on how and where waste and fraud occur.

The skilled home healthcare community has developed a package of reforms to prevent the bad actors from committing fraud and abuse. I commend the home health community for taking this stand to protect Medicare for the seniors who currently need and for future beneficiaries.



GAO
Accountability • Integrity • Reliability

**United States Government Accountability Office**
**Washington, DC 20548**

January 25, 2013

The Honorable Joseph R. Pitts
Chairman
Subcommittee on Health
Committee on Energy and Commerce
House of Representatives

Subject: Responses to Questions Following GAO Testimony Entitled *HEALTH CARE FRAUD: Types of Providers Involved in Medicare Cases, and CMS Efforts to Reduce Fraud*

Dear Mr. Chairman,

This letter responds to your January 10, 2013 request that we address your questions following the Subcommittee's November 28, 2012 hearing entitled *"Examining Options to Combat Health Care Waste, Fraud and Abuse."*

If you have any questions about the letter or need additional information, please contact me on (202) 512-7114 or at KingK@gao.gov or contact Martin Gahart, Assistant Director, on (202) 512-3596 or at GahartM@gao.gov.

Sincerely yours,

Kathleen M. King

Kathleen King
Director, Health Care

Enclosure

**Responses to Post-Hearing Questions for the Record**
**Examining Options to Combat Health Care Waste, Fraud and Abuse**

**Subcommittee on Health, Committee on Energy and Commerce**
**U.S. House of Representatives**
**November 28, 2012**

**Questions for Kathleen M. King**
**Director, Health Care**
**U.S. Government Accountability Office**

**Questions for the Record Submitted by the Honorable Joseph R. Pitts**

1. **In order for this Congress to get a handle on the existing fraud and integrity problems within the Medicare program, transparency on the part of CMS with regards to the current extent of the problem is important. Do you believe that CMS has been fully transparent with regards to its fraud and abuse efforts? If not, what can they improve upon? If so, please describe the agency's efforts to promote transparency. How can the agency increase transparency?**

   As we have previously indicated, the extent of fraud in Medicare is unknown and there are no reliable estimates of the magnitude of the problem. In the Health Care Fraud and Abuse Control program annual report to Congress for fiscal year 2011, the Centers for Medicare & Medicaid Services (CMS) indicated that it was working to develop an estimate of probable fraud in the Medicare fee-for-service program. The report noted that documenting a baseline for the amount of fraud in Medicare was critical to evaluating the success of ongoing fraud prevention activities.

   CMS has published several reports and testified in Congress on its fraud efforts. However, there have been instances where CMS has not met statutory reporting deadlines. For example, the Small Business Jobs Act of 2010 required that CMS issue a report by September 30, 2012 on the first implementation year for the Fraud Prevention System. CMS submitted that report to Congress on December 14, 2012. Additionally, the Patient Protection and Affordable Care Act of 2010 required that CMS submit an annual report to Congress on the use of funds for the Medicare Integrity Program and the effectiveness of the use of those funds. The report is due 180 days after the end of each fiscal year, beginning in fiscal year 2011. As of January 22, 2013, CMS has not submitted the fiscal year 2011 report.

   Over the last several years, GAO has completed several studies of CMS's program integrity efforts. During the course of these studies, CMS officials have been responsive to our requests for information.

2. **In its recent report on the FPS, did the GAO confirm that the FPS had ever stopped a single claim on the payment floor thereby showing this project was indeed doing what they claimed they would and "stop the pay and chase"?**

   We have not evaluated the report CMS released in December 2012 on the first implementation year. In our October 2012 report, we concluded that CMS has not yet implemented the FPS system functionality necessary to suspend payment of high-risk claims on the "payment floor" (see *Medicare Fraud Prevention: CMS Has Implemented a Predictive Analytics System, but Needs to Define Measures to Determine Its Effectiveness*, GAO-13-104 (Washington, D.C.: Oct. 15, 2012)). However, most high-risk claims will likely require investigation by analysts and fraud investigators before being denied. Specifically, CMS program integrity officials told us that the agency intends to use FPS to deny only a small number of claims without further investigation once it completes integration of FPS with its claims-payment system. CMS's program integrity analysts' use of FPS has generally been consistent with key practices for using predictive analytics identified by private insurers and state Medicaid programs. For example, publicizing the use of predictive analytics technologies may deter providers from committing fraud. However, CMS officials told us that it is difficult to determine benefits or return on the agency's investment in FPS in part because of the deterrent effect, which prevents fraudulent activity from occurring and the amount of costs avoided would be unknown.

3. **The Deputy Administrator and Director of the Center for Program Integrity, Dr. Peter Budetti, testified before the House Oversight and Government Reform Committee on April 5, 2011, and testified that most of the $60 billion in improper payments accounted for in 2010 were not "usually fraudulent nor necessarily payments for inappropriate claims" but rather indications that errors were made by the provider in filing a claim or inappropriately billing for a service. Do you agree with that statement? Please explain.**

   We agree with Dr. Budetti that many improper payments are not fraudulent. The improper payment estimate includes both overpayments and underpayments and is not designed to detect or measure the amount of fraud that may exist. Payment errors can arise from several sources, including 1) services that were not documented or where the documentation was not provided when requested, 2) services where the documentation is provided, but not sufficient, 3) services which are not correctly coded for payment, and 4) services that are not determined to be reasonable and necessary, after review of the documentation. For example, if a Medicare beneficiary has other health insurance that should be used to pay for the service, but the provider bills Medicare as the primary payer by mistake, Medicare might pay the claim and that would result in an improper payment. Similarly, a provider might have provided the service in a hospital setting, when the patient could have been treated in an outpatient setting—that would also be a payment error. In both of these examples, the service was provided to the beneficiary, but the payment Medicare made was not correct.

4. **CMS and other payers employ a series of "medical edits" which allow payers to identify inappropriate claims, and these automated systems can detect and reject payment for services that are improper or likely fraudulent, such as a hysterectomy billed for a male beneficiary. What is the extent to which the Medicare program utilizes these edits in comparison to private payers? Is there room for Medicare to improve its use of medical edits and, if so, how?**

   The Medicare program applies prepayment edits to all fee-for-service claims, but we do not know how that compares to private payers' use of edits. In our November 2012 report on prepayment edits, we found that, in fiscal year 2010, use of edits saved Medicare at least $1.76 billion, but edits could have been used even more extensively (see *Medicare Program Integrity: Greater Prepayment Control Efforts Could Increase Savings and Better Ensure Proper Payment*, GAO-13-102 (Washington, D.C.: Nov. 13, 2012)). For example, we found $14.7 million in payments that appeared to be inconsistent with national policies, such as national coverage decisions and nationally-implemented medically unlikely edits. Such payments could have been avoided through more extensive use of edits. In addition, more widespread use of local edits developed by Medicare Administrative Contractors in their jurisdictions could also lead to savings. We also found some weaknesses in the processes for determining the need for and implementing edits, such as the process of addressing vulnerabilities to improper payment identified by Recovery Auditing Contractors. As a result, we made several recommendations to the CMS Administrator to promote implementation of effective edits based on national policies and to encourage more widespread use of effective local edits by Medicare Administrative Contractors.

5. **You testified that GAO is currently assessing prepayment medical edits in Medicare and CMS's oversight of its contractors and implementing those edits to help ensure Medicare pays claims correctly the first time. Please explain the report's methodology and provide a timeline for the report that includes the planned date of completion.**

This report was released on December 10, 2012 (GAO-13-102). In the report, we assessed the use of prepayment edits in the Medicare program and CMS's oversight of Medicare administrative contractors (MACs), which process claims and implement some edits. Our report examined the extent to which (1) CMS and its contractors employed prepayment edits, (2) CMS has designed adequate processes to determine the need for and to implement edits based on national policies, and (3) CMS provides information, oversight, and incentives to MACs to promote use of effective edits. We analyzed Medicare claims for consistency with selected coverage policies, reviewed CMS and contractor documents, and interviewed officials from CMS and selected contractors. Additional details on our methodology are available in our report.

6. **Many of the witnesses who testified emphasized the importance of staying abreast of new and emerging frauds and an adaptable system of prevention to address these concerns. You mentioned in your testimony the need for CMS to develop a robust process for identifying vulnerabilities in the Medicare program. How does CMS currently assess vulnerabilities in the program?**

CMS's Vulnerability Tracking Corrective Action Process began in November 2008. It was originally developed to track vulnerabilities identified by Recovery Auditing Contractors and corrective actions taken, but it has expanded to include vulnerabilities identified through other means. CMS has designed a process that calls for analyzing several sources of information—such as payment error rate data and data on improper payments identified by CMS contractors—in order to identify potential vulnerabilities. CMS staff then assess the risks posed by these vulnerabilities and prioritize them for corrective action based on several criteria, including whether the vulnerability has been identified as a "major finding," meaning a vulnerability for which more than $500,000 was identified for recoupment, the overall financial impact, and the geographic impact and scope. The agency has assembled a Corrective Action Development Team, which meets weekly to review analyses on prioritized vulnerabilities and to propose corrective actions to leadership in the CMS Provider Compliance Group, which is responsible for vulnerability tracking. The Provider Compliance Group can develop edits or take other corrective actions such as publishing provider education articles, referring vulnerabilities to other CMS components, or referring vulnerabilities to the MACs to be addressed at the local level.

In our November 2012 report on prepayment edits (GAO-13-102), we identified two weaknesses in the process related to assessing vulnerabilities and having timeframes and monitoring activities for addressing them. As a result, we recommended that the CMS Administrator revise the method for compiling information about recovery-auditor-identified vulnerabilities to identify their full extent and prioritize them accordingly, and develop written procedures to provide guidance to agency staff on all steps in the processes for developing and implementing edits based on national policies.
HHS generally concurred with our recommendations and cited actions that CMS plans to take to address them.

7. **CMS currently has a number of contractors they work with to ferret out waste, fraud and abuse. Many of these contractors have protocol in place to share their findings about new and emerging fraud trends with CMS. In your testimony, you cite the need to improve the use of existing technologies that could help CMS and contractors identify fraud not only after claims have been paid but before as well and go on to cite the Fraud Prevention System as one technology that can help CMS identify fraud before claims are paid. Are there other examples that you can share with this committee?**

   We believe there are a number of ways to better leverage the substantial investment that CMS has already made with FPS. This includes continuing to expand the number and complexity of predictive analytic models used by FPS to detect different types of fraudulent behavior and adding tools to FPS to help detect more elaborate fraud schemes. For example, CMS has plans to integrate social network analysis, an emerging and important tool to combat organized health care fraud since it can be used to demonstrate linkages among individuals involved in fraud schemes. CMS currently has a modeling contract with International Business Machines (IBM) Corporation to help in these endeavors. In addition, CMS should, as we recommended in our report (GAO-13-104), implement functionality in the FPS system needed to suspend payment of high-risk claims and develop the detailed project schedules necessary to accomplish this effort. CMS can also better use FPS to address broader program integrity vulnerabilities within Medicare. Private insurers and state Medicaid programs we interviewed that use predictive analytics reported that they use predictive analytics to identify and close prepayment edit gaps and coverage policy loopholes that are exploited by providers for fraud, such as lack of utilization limits for certain services. In addition to improving the use and functionality of FPS, CMS needs to determine ways to define and measure financial benefits of using FPS. Until such performance indicators are established for FPS, CMS officials will continue to lack the information needed to determine FPS's overall effectiveness as a technology in preventing fraudulent behavior, and how it compares to other program integrity efforts to reduce Medicare fraud.

8. **You testified that GAO made recommendations to CMS on ways to improve their fraud prevention activities. Please submit a list all of the recommendations you have made over the past 5 years and the extent which CMS has implemented those recommendations.**

   Table 1 provided below was also provided to the Subcommittee separately on January 11, 2013.

**Table 1: List of Open Program Integrity Recommendations Made by GAO to the Centers for Medicare and Medicaid Services (CMS), Fiscal Years 2009 through 2012**

| Product Number | Product Title | Issue Date | GAO Recommendation |
|---|---|---|---|
| GAO-09-185 | Medicare: Improvements Needed to Address Improper Payments in Home Health | 2/27/2009 | To strengthen the controls on improper payments in the Medicare home health benefit, the Administrator of CMS should amend current regulations to expand the types of improper billing practices that are grounds for revocation of billing privileges. Grounds for revocation could include a pattern of submitting claims that are falsified, for persons who do not meet Medicare's coverage criteria, or for services that are not medically necessary. |
| GAO-09-185 | Medicare: Improvements Needed to Address Improper Payments in Home Health | 2/27/2009 | To strengthen the controls on improper payments in the Medicare home health benefit, the Administrator of CMS should direct CMS contractors to conduct postpayment medical reviews on claims submitted by HHAs with high |

| | | | |
|---|---|---|---|
| | | | rates of improper billing identified through prepayment review. |
| GAO-10-143 | Medicare Recovery Audit Contracting: Weaknesses Remain in Addressing Vulnerabilities to Improper Payments, Although Improvements Made to Contractor Oversight | 3/31/2010 | To help reduce future improper payments, the Administrator of CMS should develop and implement a process that includes policies and procedures to ensure that the agency promptly: (1) evaluates findings of RAC audits, (2) decides on the appropriate response and a time frame for taking action based on established criteria, and (3) acts to correct the vulnerabilities identified. |
| GAO-11-592 | Medicare Integrity Program: CMS Used Increased Funding for New Activities but Could Improve Measurement of Program Effectiveness | 7/29/2011 | To enhance accountability and sharpen the focus of the agency on reducing improper payments, the Administrator of CMS should clearly communicate to staff the linkage between Government Performance and Results Act (GPRA) and Patient Protection and Affordable Care Act (PPACA) performance measures related to the reduction in improper payments and other measures used to determine the performance of Medicare Integrity Program (MIP) activities. |
| GAO-11-592 | Medicare Integrity Program: CMS Used Increased Funding for New Activities but Could Improve Measurement of Program Effectiveness | 7/29/2011 | To enhance the reliability of data used to calculate the MIP retum on investment (ROI), the Administrator of CMS should expeditiously complete the implementation of data system changes that will permit CMS to capture accurate Medicare administrative contractor (MAC) spending data, thereby helping to ensure an accurate ROI. |
| GAO-11-592 | Medicare Integrity Program: CMS Used Increased Funding for New Activities but Could Improve Measurement of Program Effectiveness | 7/29/2011 | To enhance the reliability of data used to calculate the MIP ROI, the Administrator of CMS should periodically update ROI calculations after contractor expenses have been audited to account for changes in expenditure data reported to CMS and publish a final ROI after data are complete. |
| GAO-12-627 | National Medicaid Audit Program: CMS Should Improve Reporting and Focus on Audit Collaboration with States | 6/14/2012 | To effectively redirect the NMAP toward more productive outcomes and to improve reporting under the DRA, the CMS Administrator should ensure that the Medicaid Integrity Group's (MIG) future annual reports to Congress clearly address the strengths and weaknesses of the audit program and its effectiveness. |
| GAO-12-627 | National Medicaid Audit Program: CMS Should Improve Reporting and Focus on Audit Collaboration with States | 6/14/2012 | To effectively redirect the NMAP toward more productive outcomes and to improve reporting under the Deficit Reduction Act of 2005 (DRA), the CMS Administrator should ensure that the MIG's planned update of its comprehensive plan (1) quantifies the NMAP's expenditures and audit outcomes; (2) addresses any program improvements; and (3) outlines plans for effectively monitoring the NMAP program, including how to validate and use any lessons learned or feedback from the states to continuously improve the audits. |
| GAO-12-627 | National Medicaid Audit Program: CMS Should Improve Reporting and Focus on Audit Collaboration with States | 6/14/2012 | To effectively redirect the NMAP toward more productive outcomes and to improve reporting under the Deficit Reduction Act of 2005 (DRA), the CMS Administrator should ensure that the MIG's use of NMAP contractors supports and expands states' own program integrity audits, engages additional states that are willing to participate in collaborative audits, and explicitly considers state burden when conducting audit activities. |
| GAO-12-831 | Medicare: CMS Needs an Approach and a Reliable Cost Estimate for Removing Social Security Numbers from Medicare Cards | 8/1/2012 | In order for CMS to implement an option for removing SSNs from Medicare cards, the Administrator of CMS should develop an accurate, well-documented cost estimate for such an option using standard cost-estimating procedures. |

| | | | |
|---|---|---|---|
| GAO-12-831 | Medicare: CMS Needs an Approach and a Reliable Cost Estimate for Removing Social Security Numbers from Medicare Cards | 8/1/2012 | In order for CMS to implement an option for removing SSNs from Medicare cards, the Administrator of CMS should select an approach for removing the SSN from the Medicare card that best protects beneficiaries from identity theft and minimizes burdens for providers, beneficiaries, and CMS. |

Note: The table includes only recommendations not implemented by CMS. Recommendation status updated in September 2012.

HEALTH
INFORMATION
DESIGNS

Health Information Designs, LLC
391 Industry Drive
Auburn, Alabama 36832

January 25, 2013

The Honorable Joseph R. Pitts
Chairman
Subcommittee on Health
United States House of Representatives
Washington, DC 20515-6115

Dear Chairman Pitts:

Enclosed please find my responses to questions for the record arising from my appearance before the Committee on November 28, at the "Examining Options to Combat Health Care Waste, Fraud, and Abuse" hearing. I hope that this information is of assistance to the Committee.

Please do not hesitate to contact me if I can be of further assistance.

Sincerely yours,

Dan Olson, CFE
Director of Fraud Prevention

Enclosure (1)

cc: The Honorable Frank Pallone, Jr.
Ranking Member

**Questions for the Record**
**Dan Olson, CFE**
**Subcommittee on Health**
**United States House of Representatives**
**November 28, 2012**

**QUESTIONS POSED BY CHAIRMAN PITTS**

**1a. In your recommendations on ways to improve fraud prevention activities within Medicare, you mention increased support for the Medicare Fraud Strike Force. What steps would you recommend we take to expand the Medicare Fraud Strike Force?**

**Response:**

The Medicare Fraud Strike Force recorded the single largest healthcare fraud recovery in history during FY 2011—over $4 billion dollars.[1] This accomplishment demonstrates that a dedicated partnership can achieve success in fighting healthcare fraud and abuse. The Medicare Fraud Strike Force is currently operating in nine metropolitan cities nationwide.[2]

The Medicare Fraud Strike Force can achieve continued and expanded success by implementing the following steps:

- **Continue to expand the discretionary Health Care Fraud and Abuse Control (HCFAC) program investments that are allocated to the Medicare Fraud Strike Force.** The FY 2013 discretionary budget that funds the Medicare Fraud Strike Force is $610M. The conservative Return on Investment (ROI) is $1.50 for every $1 spent.[3] Additional dollars allocated to the Medicare Fraud Strike Force will increase the identification of frauds committed against the Medicare program and increase the overall ROI.
- **Expand the number of Medicare Fraud Strike Forces into additional major metropolitan areas.** Additional dollars allocated to the Medicare Fraud Strike Force will promote the expansion into additional major metropolitan areas. Expansion efforts will continue to establish a wider net to capture and prosecute criminals, increase the monetary recoupments, and improve the ROI. These efforts will also lead to an increase in the sentinel effect and promote cost avoidance on the front end rather than pay and chase on the back end.
- **Expand the composition of the Medicare Fraud Strike Force beyond Health and Human Services (HHS), Department of Justice (DOJ), Office of Inspector General (OIG) and the Federal Bureau of Investigation (FBI).** The addition of the Drug Enforcement Agency (DEA) and their Organized Crime Drug Enforcement Task Force, Internal Revenue Service (IRS), and the state licensure agencies will provide the Medicare Fraud Strike Force with partners that can identify criminal networks involved in kickback schemes, money laundering, illicit drug activity, and tax evasion.
- **Coordinate the work of the Medicare Fraud Strike Force with other CMS contractors.** The criminal mind is constantly looking for new ways and methods to take advantage of the payer's system. To combat the criminal effort, the Medicare Fraud Strike Force should be enhanced by leveraging the ongoing healthcare fraud work conducted by CMS contractors, including Zone Program Integrity Contractors, Recovery Audit Contractors, and Medicare Drug Integrity Contractors. Linking the data stores and data analysis techniques employed by these contractors with the investigative and prosecution actions taken by the Medicare Fraud Strike Force will expedite the identification of emerging trends, abusive payment patterns, aberrant claims, and fraud hotspots before the perpetrator(s) exploit the system.

**1b. What steps would you recommend we take to create Medicaid Fraud Strike Forces at the State level?**

**Response:**

Creation of new Medicaid Fraud Strike Forces, which would operate at the State level, would improve the identification and collection of dollars lost to healthcare fraud, waste, and abuse. Implementation of the following steps will facilitate the implementation of the Strike Forces at the State level:

- **Establish a collective membership for each Medicaid Fraud Strike Force that includes the following entities: State Medicaid Agency, Medicaid Fraud Control Unit, Attorney General, District Attorney, FBI, DEA, IRS, Professional Licensing Boards, Vital Records, and contractual subject matter experts.** The membership includes state-level entities that mirror those on the Medicare Fraud Strike Force. The membership is strengthened through the inclusion of additional regulatory agencies that will assist in the identification of criminal networks involved in kickback schemes, money laundering, illicit drug activity, and tax evasion.
- **Execute Data Sharing Agreements among all task force entities.** Data analysis is central to the identification of emerging patterns and trends that indicate potential fraud and abuse. The removal of data barriers is a prerequisite to ensuring full, free, unrestricted access to data and therefore promoting detailed claim analysis. The absence of this critical component opens doors for the criminal element and promotes their continued abuse of the Medicaid payer's system.
- **Produce an annual report of the activity completed by the Medicaid Fraud Strike Force.** Precedent has been established for this type of report through CMS' Medicaid Integrity Program Comprehensive Program Integrity Reviews annual report.[4] This report highlights noteworthy practices, effective practices and weaknesses identified in the program that can then be emulated by the Medicare Fraud Strike Force and other Medicaid Fraud Strike Forces.
- **Obtain enhanced Federal Financial Participation (FFP) matches to support any pilot project undertaken by the Medicaid Fraud Strike Force.** CMS provides states a 90 percent FFP match for the design, development, installation and enhancement of new Medicaid eligibility systems and 75% for the maintenance and operation of the system. Enhanced FFP will provide each Medicaid Fraud Strike Force with the ability to dedicate the necessary resources to effectively ferret out fraud and abuse in their Medicaid programs in a more comprehensive manner.
- **Establish the respective regional CMS office as the governing entity for each Medicaid Fraud Strike Force.** The ten regional CMS offices with oversight by the Consortium for Medicaid and Children's Health Operations (CMCHO) will provide an existing reporting structure for each Medicaid Fraud Strike Force. The CMCHO will provide uniform issue management, consistent communication and leadership focused on achieving CMS strategic action plan. The Consortium Administrator for CMCHO will serve as the agent that is responsible for consistent implementation of the Medicaid Fraud Strike Force, and policy and guidance across all ten regions to advance the mission of each Strike Force.
- **Create a repository to store all task force annual reports, established and maintained by CMS.** A singular point of entry to access the annual reports of each Medicaid Fraud Strike Force will facilitate the sharing of states' best practices.

The following entities will benefit through the implementation of the Medicaid Fraud Strike Force:

- CMS will benefit through an expedited implementation and adoption of the Medicaid Fraud Strike Force due to the existing structure of the Medicare Fraud Strike Force and oversight provided by the CMCHO and the ten regional CMS offices.
- State Medicaid agencies will benefit through data sharing and the identification of emerging patterns and trends.
- Medicare will benefit through regionalized issues raised and vetted at the state level and presented as actionable items at the federal level.

**2a. What steps would you take to help ensure the proper implementation of the Integrated Data Repository?**

**Response:**

In July 2011, the General Accounting Office (GAO) issued a report entitled *Fraud Detection Systems: Additional Actions Needed to Support Program Integrity Efforts at Centers for Medicare and Medicaid Services*.[5] The report showed that the Integrated Data Repository (IDR) has been only partially rolled out and that Medicaid data has not been incorporated into the system. CMS recently established the Medicaid and CHIP Business Information Solution (MACBIS) Council to develop a strategy to improve the quality and consistency of the data reported to the Federal government from each State.

The following steps would facilitate the implementation of the IDR so that Medicare and each Medicaid state agency can utilize it to perform data analytics:

- **Develop regionalized IDRs consistent with the ten CMS regions.** Aligning the IDRs consistently with the existing CMS regions will take advantage of the existing infrastructure and minimize the disruption that a new initiative creates. The lessons learned from each regional IDR will promote a smoother and more rapid transition to the federal IDR.
- **Maintain the data protocols developed for the federal IDR and mirror them in each regional IDR.** Consistency in the data protocols will minimize disruption when successful applications at the regional level are migrated for testing and implementation into the federal IDR.
- **Restrict the initial regionalized federal and state data loads by adopting the following approach**:
  - Roll out the claim-level data one date of service year at a time until testing is complete. Multiple state Medicaid data sources require the normalization of the data so that it can satisfy a singular source for information reporting requirements. Processing the data loads on a yearly basis within each regionalized area will more rapidly identify issues and promote a quicker resolution so that further testing and data loads can occur.
  - Roll out the claim-level data by provider type to ensure the system is functioning properly. For example, the initial data load for each region should only include physician data. The IDR system architecture, underlying data transformations, and system logic are very complex. Evaluating the system by provider type will allow appropriate testing to identify issues and resolve them before introducing an additional provider type.
  - Roll out the claim-level data within a minimum data set (MDS). For example, the MDS would include up to 20 claim-level data items that can be used to evaluate the accuracy of the data transfer to each regional IDR and the output that is generated from the IDR. Continually expand the variables in the MDS after satisfactory testing has been completed for the previous MDS. This iterative process will allow appropriate testing to identify issues and resolve them before introducing additional variables.

- **Conduct testing and training of each regionalized IDR with a cross-section of federal, state, and contractual subject matter experts.** Testing by a cross-section of subject matter experts from multiple disciplines and backgrounds will strengthen the testing process and speed the adoption of the IDR so that both Medicare and each Medicaid state agency can utilize it.

The benefits achieved through a regionalized approach to development include a more rapid development and a shortened testing and training cycle. The regionalized approach will promote a smoother transition to the federal IDR and therefore maximize the benefits obtained at the Medicare and Medicaid levels.

**2b. Why is this so critical to the success of fighting healthcare fraud?**

**Response:**

The implementation of the IDR for use by Medicare and state Medicaid agency staff has the potential to reinvent the manner in which healthcare data analytics are utilized. Breaking down existing Medicare and Medicaid data silos and moving all data into a seamless integrated system will advance the cause of healthcare fraud prevention and elevate the analysis of Medicare and Medicaid claims data to a new level.

Data analytics are at the heart of identifying patterns and trends in healthcare data. Consolidation of Medicare and Medicaid data into a single IDR will remove barriers that hinder existing analysis of data so that predictive analytics and other more sophisticated types of analysis can be conducted. The IDR will provide the Medicare and Medicaid healthcare analyst a richer and more comprehensive dataset to evaluate data on a national scale. The IDR will enhance the work of all healthcare fraud programs, including the Fraud Prevention System (FPS), and provide the Medicare and Medicaid Fraud Strike Forces actionable results that they can use to investigate and prosecute healthcare fraud criminals.

**3. You mentioned in your testimony how useful the calculating and publishing of national and state-wide healthcare statistics would be for fraud prevention. Why is it so critical to establish baseline thresholds and publish them?**

**Response:**

The DOJ, FBI, and OIG are using advanced data analysis techniques to evaluate healthcare claims. One technique, known as anomaly-detection, identifies healthcare fraud "hot spots" so that analysts can target emerging fraud schemes. Anomaly-detection of a healthcare fraud hot spot occurs when a provider's claim volume exceeds a provider billing pattern that has been established and determined to be reasonable. For example, on February 28, 2012 a Texas physician and several accomplices were arrested in a nearly $375 million healthcare fraud scheme that was identified due to a fraud hot spot. The fraud analysts discovered that in 2010, while 99 percent of physicians who certified patients for home health signed off on 104 or fewer people, the indicted physician certified more than 5,000 individuals.[6]

The GAO reports that the FPS relies on historical data to develop the three models currently in use.[7] The thresholds calculated from historical data are used in the FPS anomaly-detection models and predictive models to indicate potential abuse that warrant analysis and investigation by the appropriate law enforcement body.

The establishment and publication of Medicare and Medicaid fraud hot spots will provide healthcare fraud data analysts with insights into state and national standards to develop data models and determine if potential abuses are occurring. Implementation of the following steps will provide healthcare fraud data analysts with additional information to uncover emerging schemes.

- **Establish baseline thresholds by provider type at the Medicare and Medicaid level.** Provider type thresholds will serve as the peer groups for anomaly-detection models. The thresholds within provider type should be based on national standard groupings, e.g., Current Procedural Terminology Manual, International Classification of Diseases Manual Version 9 or National Drug Codes.
- **Update the threshold list quarterly.** Regular updates to the thresholds will ensure that the claims data will capture new or emerging trends exhibited in the data set. Regular updates will also provide the healthcare data analyst with the ability to evaluate current data trends against provider patterns that have been established and determined to be reasonable.
- **Publish the threshold list on the CMS website.** Publication will provide ready data access to Medicare and Medicaid healthcare data analysts so that they can evaluate their data against state and national standards to determine if potential abuse is occurring.

4. **You mention in your testimony how important it would be to match vital records to SSA and State programs. Can you further define your recommendation to incorporate vital records information at both the federal and state level?**

**Response:**

On July 9, 2008, the Senate Subcommittee on Investigations released a report showing that between $60 million and $92 million was paid to Medicare recipients by deceased Medicare providers.[8] On September 30, 2009, the GAO released a report showing that over $700,000 was paid for controlled substances on behalf of deceased Medicaid recipients or prescribed by deceased Medicaid providers.[9] Both reports reveal weaknesses in the system currently used to maintain provider and recipient date of death information.

Implementation of the following steps will improve the accuracy of the federal and state date of death information:

- **Establish a nightly data feed of accurate provider and recipient date of death information to the Social Security Administration (SSA) Death Match File (DMF) and the state Medicaid Management Information System (MMIS).** The death match information will establish the basis for an edit to reject any claims presented for payment after the recipient or provider's date of death.
- **Establish an edit that matches the claim date of service against the provider or recipient date of death to determine the validity of the claim.** Reject the claim if the date of service exceeds the date of death. Perform an analysis to recoup improper payments after the date of death.
- **Require a death indicator to be placed on the recipient's file or the provider's identification number when death notice is given and pend all claims until a date of death can be validated.** Perform an analysis to recoup improper payments paid prior to the death indicator being placed on the file. Reject future claims received after the valid date of death has been established.
- **Periodically cleanse the active recipient database by performing a cross-match of all eligible recipients against the SSA DMF and MMIS.** Perform an analysis to identify all claims paid after the recipient's date of death and establish a recoupment process to recover improper payments.
- **Periodically cleanse the active provider file by performing a cross-match of all active providers against the SSA DMF and MMIS.** Perform an analysis to identify all claims paid after the provider's date of death and establish a recoupment process to recover improper

payments. This type of fraud scheme is typically indicative of a larger scheme where the perpetrator has obtained an older provider ID and begun submitting false claims.

Accurate and up-to-date recipient and provider date of death data will allow Medicare and Medicaid claims to be rejected at point of submission rather than after the claim is paid (the standard "pay and chase" model).

5. **In 2010, then Acting Deputy Attorney General Gary Grindler stated that "it is not enough just to prosecute and punish health care fraud after it occurs. We must target it before it happens through aggressive pre-screening, auditing, and prevention techniques." An all of the above strategy if you will. While much public attention has been given to post payment recovery efforts under this Administration, do you believe that we are doing enough in aggressive pre-screening and prevention techniques?**

**Response:**

I believe that we can and must do additional work to improve pre-screening and fraud prevention techniques. The current actions being implemented through the provider screening program and the FPS hold promise to enhance our fight against healthcare fraud, waste and abuse. However, healthcare fraud is dynamic—not static. The criminal mind is constantly looking for new ways and methods to take advantage of the payer's system. It is incumbent on the fraud control professional to continually expand beyond our existing efforts or risk falling prey to new schemes perpetrated against the Medicare and Medicaid programs.

Fraud expert Dr. Malcolm Sparrow points out that the compelling nature of fraud control demands vigilance, unpredictability, and sabotage in responding to emerging patterns of fraud.[10]

- **Vigilance** – Fraud control professionals must be vigilant—ever-seeking new possibilities or angles that allow fraud and abuse to be identified as it is occurring and before the claim is paid.
- **Unpredictability** – Fraud control professionals must alter and vary their analysis techniques to keep their detection methods unpredictable to create an imbalance for fraud perpetrators that will confuse and possibly defuse their planned fraudulent activities.
- **Sabotage** – Fraud control professionals must be nimble, in order to counteract emerging fraud and abuse schemes by sabotaging them early in their development.

While each of these factors is significant individually, the combination of the three produces the best possible climate for identifying cases of fraud and abuse and potential acts of fraud and abuse. Fraud control professionals should work diligently to achieve this optimal environment. We must leverage the power of data analytics and statistical profiling, and collaborate with stakeholders and law enforcement, to provide an intentional vigilance in our mission to combat and disrupt emerging issues in healthcare fraud and abuse.

Implementation of the following steps will help to expand the existing pre-screening and prevention programs:

- **Conduct background checks on all newly enrolled providers.** On March 25, 2011, CMS strengthened the provider enrollment process by expanding Sections 19 – 19.4, Chapter 15 of the *Medicare Program Integrity Manual.*[11] The *Medicare Program Integrity Manual* requires newly enrolled providers to be evaluated and then monitored based on one of the following three risk levels: limited, moderate, or high. Providers classified as limited or moderate are not subject to a criminal background check. This assumption incorrectly presupposes that providers classified as limited or moderate are not likely to commit fraud. The absence of a criminal background check for providers classified as limited or moderate opens a loophole to potential fraud or abuse.

- **Enact a mandatory provider re-enrollment program to be implemented by all Medicaid agencies.** The Medicaid re-enrollment program will complement the Medicare re-enrollment program and will provide the following significant benefits:
  - Removal of non-existent, inactive, retired, or deceased providers from the Medicaid rolls
  - Validation and update of professional licensure information for each active provider
  - Validation and update of provider demographic information
  - Validation and update of respective provider databases with current information
- **Monitor growth patterns for newly enrolled providers.** Typically, the expected growth pattern for a newly enrolled provider would be a gradual increase in their claim volume, number of recipients seen per day, total dollars paid, etc. Performing anomaly-detection to compare the growth pattern of a newly enrolled provider against their peer group's growth pattern will identify abnormal billing patterns. The abnormal billing patterns may indicate a bust-out scheme, for example false claims submitted through a loophole that is being exploited.
- **Implement surety bond requirements for all newly enrolled providers.** Medicare currently requires surety bonds for Suppliers of Durable Medical Equipment, Prosthetics, Orthotics, and Supplies and Home Health agencies. Expanding the requirement to all newly enrolled providers will add a deterrent effect on would-be fraudsters. The surety bond will:
  - Limit the Medicare program risk to fraudulent suppliers
  - Enhance the legitimacy of the Medicare enrollment process and current suppliers
  - Ensure the Medicare program is indemnified for erroneous payments resulting from fraudulent or abusive supplier billing practices
  - Ensure Medicare beneficiaries receive reasonable products and services from legitimate suppliers[12]
- **Develop predictive models that are based on quality of care issues.** Accountable Care Organizations (ACOs) provide coordinated care to Medicare recipients with the goal of avoiding unnecessary duplication of services and preventing medical errors.[13] Coordination of care improves the recipient's outcome and achieves savings for the Medicare program. Additional savings can be generated through the development of predictive models that calculate risk-scores based on quality of care indexes that predict future hospitalizations or hospital re-admissions. The quality of care indexes would be derived from medical conditions presented during office visits, consultations or previous institutional care.

**6a. Please provide the committee with a list of the fraud prevention areas that you believe could be improved within CMS. If these areas include deficiencies on the part of CMS, can you provide explanation as to why you believe those deficiencies exist?**

**Response:**

The following areas can be improved within CMS:

- **Medicare and Medicaid Partnership.** Expand cooperative efforts between Medicare and Medicaid. The National Association for Medicaid Directors (NAMD) sent a letter to CMS on October 6 requesting that CMS engage with states in a number of concrete activities.[14] NAMD also expressed a desire for more thorough and sustainable integration of Medicaid program integrity with related CMS efforts. The letter encourages CMS to adopt Medicaid as a full partner in federal/state initiatives.

NAMD requests assistance from CMS in the following four areas to improve Medicaid Program Integrity activities:

- Federal and State Collaboration
- Fraud Investigations Database
- Provider Screening and Verification
- Medicaid Integrity Contractors Data

The benefits achieved when Medicare and Medicaid are full partners include:

- Improving the communication between Medicare and Medicaid regarding healthcare fraud and abuse issues and initiatives
- Improving the effectiveness and adoption of Medicare and Medicaid initiatives
- Improving the sharing of data for Medicare and Medicaid programs and initiatives
- Improving the results of data analysis and best practices to address emerging healthcare fraud trends and patterns

➢ **Do Not Pay List.** Expand the "Do Not Pay List" to include retired or sanctioned DEA numbers. On June 18, 2010, a presidential memorandum was issued titled *Enhancing Payment Accuracy Through a "Do Not Pay List."* The memorandum ordered the creation of a centralized database that federal agencies will be required to search before distributing payments to contractors and providers. The "Do Not Pay List" was prompted by a three-year report from federal auditors that revealed that federal agencies paid $180 million in benefits to 20,000 deceased individuals and over $230 million to about 14,000 fugitives or incarcerated felons who are ineligible for benefits.[15]

The DOJ, Office of Drug Diversion maintains a file of all practitioners who have been assigned a DEA number. The file is updated monthly with new DEA registrants, reinstated DEA numbers, and retired DEA numbers.

The following data integrity benefits will be achieved by performing a cross-match of the data in the Medicare/Medicaid claim and DEA registry:

- Validate the DEA number submitted on the claim by cross-matching it to the DEA registry
- Confirm that the DEA number is active on the DEA registry prior to paying the claim
- Confirm that the DEA registrant has permission to dispense prescriptions in the state of origin on the claim
- Provide the identity of the prescriber for those instances where the prescriber is not enrolled by Medicare or Medicaid
- Identify claims submitted with inappropriate controlled substance authority
- Identify claims submitted with an expired or retired DEA number

➢ **Home Health Surety Bonds.** Establish procedures to implement the surety bond requirement for Home Health Agencies (HHAs). CMS issued a rule[16] in January 1998 that requires each HHA to obtain a surety bond in the amount of $50,000 or 15 percent of the annual amount paid to the HHA by Medicare, whichever is greater.

The HHS OIG released the following report in September 2012: *Surety Bonds Remain an Unused Tool to Protect Medicare from Home Health Overpayments.* OIG found that "as of February 29, 2012, 2,004 HHAs still owed CMS a total of approximately $408 million for $590 million in overpayments that the agency identified for these HHAs between 2007 and 2011. CMS could have recovered at least $39 million between 2007 and 2011 if it had required each HHA to obtain a $50,000 surety bond. Of the 2,004 HHAs, 21% still had overpayment amounts, excluding interest, of more than $50,000 each, and more than a quarter of these HHAs had outstanding overpayments of greater than $500,000."

The report recommends that CMS implement the HHA surety bond requirement, and it adds a new recommendation: "To recoup a higher percentage of overpayments made to HHAs, CMS should consider increasing surety bond amounts above $50,000 for those HHAs with high overall Medicare payment amounts."[17] Implementation of this recommendation will deter additional overpayments in the Medicare and Medicaid programs.

**6b. Can you also provide recommendations on ways that CMS fraud prevention can be improved?**

**Response:**

Fraud prevention can be improved by implementation of the following steps:

- **Establish a Medicare and Medicaid fraud think tank.** The think tank will be comprised of federal, state and contractual healthcare fraud subject matter experts in data analytics, predictive modeling and policy analysis. The goal of the think tank will be to develop new algorithms and data models to uncover emerging trends in healthcare fraud and abuse. The think tank will have full, free, unrestricted access to data and therefore promote a more rapid development cycle. Successful algorithms and data models will be published and made available to public and private healthcare entities to address emerging healthcare fraud patterns and trends.
- **Establish an ownership database that stores ownership information for each provider who owns five percent or more of the provider entity.** The deceptive nature of fraud expands through complex relationships and multiple layers of individuals and entities that seek to protect the criminal element. Often, the conduit of the abuse remains two or more steps removed from the perpetrator. Creation of the database will provide the ability for the Medicare and Medicaid healthcare data analyst to perform link analysis. Link analysis is a data analysis technique that identifies relationships between providers, recipients, and billing entities. This technique will assist healthcare analysts, investigators and prosecutors in the identification of owners: involved in a criminal network, terminated from the Medicare or Medicaid program, under investigation, etc.
- **Continue to support the efforts of the Healthcare Fraud Prevention Partnership (HFPP).** The HFPP is a new initiative that combines the resources and expertise of federal and state officials, private health insurance organizations and other healthcare anti-fraud groups. The goal of the partnership is to "perform sophisticated analytics on industry-wide data that will detect and predict fraud schemes that were previously undetectable in a fragmented healthcare system." [18] HFPP has established an Executive Board and the following two committees to oversee the initiative: Data Analysis and Review Committee (DARC) and the Information Sharing Committee (ISC). The initial challenges that are facing HFPP include privacy act concerns, HIPAA concerns, receipt of data from multiple programs, and sharing the results of the data analysis. CMS cooperative support in addressing these initial challenges will provide the HFPP initiative with the ability to achieve the following successes:
  - Expanded data set will be available for data analysis among all payers
  - Anti-fraud information will be shared among all payers
  - Investigators, prosecutors, policymakers and other stakeholders will have a more complete view of aberrant providers activity across multiple payers
  - Historical trends and patterns exhibited across industry-wide healthcare data for all providers will enhance predictive models and their ability to identify emerging trends and promote fraud prevention.

- **Establish quarterly prescriber reports that document recipient controlled substance utilization.** The 2011 National Health Expenditures (NHE) report indicates that retail prescription drug spending grew 2.9 percent to $263.0 billion.[19] Prescription drug abuse continues to permeate our society. One form of abuse occurs when a prescriber's DEA number is compromised and exploited by the fraudster through the submittal of claims using the prescriber's DEA number without their knowledge. Producing a quarterly prescribing report for each DEA number that is assigned to the prescriber will place the prescriber on notice regarding the prescriptions that have been billed under their DEA number. The report should be HIPAA-compliant and contain the details of each controlled substance paid under the prescriber's DEA number for the recipient. The following benefits will be achieved through this report:
  - Prescriber will validate their active DEA numbers
  - Prescriber will validate the recipients billed during the past quarter
  - Prescriber will validate the controlled substances billed during the past quarter
  - Prescriber will have the ability to notify authorities if false billings are identified
- **Establish a healthcare fraud analyst certification program.** The sophisticated healthcare criminal utilizes multiple methods and schemes to avert the static edits that exist in the standard claims processing system. Healthcare fraud business models are expanding beyond the business rule driven "pay and chase" model and include complex algorithms, predictive models, link analysis, etc. The healthcare analyst needs to have a well-rounded background to properly address the methods employed by the healthcare criminal. In September 2007, CMS' Medicaid Integrity Group established the Medicaid Integrity Institute (MII). "The mission of the MII is to provide effective training tailored to meet the ongoing needs of state Medicaid Program Integrity employees, with the goal of raising national program integrity performance standards and professionalism."[20] MII provides a platform for the certification program that will equip the staff person to identify potential fraud and abuse through the advanced techniques. Establishment of a certification program for Medicare and Medicaid healthcare analysts will ensure that the analyst has a baseline training to address new and emerging healthcare fraud schemes perpetrated by the healthcare fraud criminal.

[1] http://www.justice.gov/iso/opa/ag/speeches/2012/ag-speech-120214.html

[2] http://www.justice.gov/iso/opa/ag/speeches/2012/ag-speech-1210042.html

[3] http://www.hhs.gov/budget/budget-brief-fy2013.pdf

[4] http://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/FraudAbuseforProfs/Downloads/2012pisummary.pdf

[5] http://www.gao.gov/new.items/d11822t.pdf

[6] http://www.hhs.gov/news/press/2012pres/02/20120228d.html

[7] http://www.gao.gov/assets/650/649537.pdf

[8] http://www.hsgac.senate.gov/search/?q=deceased+doctors&search-button=Search&access=p&as_dt=i&as_epq=&as_eq=&as_lq=&as_occt=any&as_oq=&as_q=&as_sitesearch=&client=hsgac&sntsp=0&filter=0&getfields=&lr=&num=15&numgm=3&oe=UTF8&output=xml_no_dtd&partialfields=&proxycustom=&proxyreload=0&proxystylesheet=default_frontend&requiredfields=&sitesearch=&sort=date%3AD%3AS%3Ad1&start=0&ud=1

[9] http://www.gao.gov/new.items/d091004t.pdf

[10] Sparrow, Malcolm K. The Character of Harms: Operational Challenges in Control. Cambridge University Press, 2008

[11] https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNMattersArticles/downloads/MM7350.pdf

[12] http://www.alphasurety.com/Surety-Bond-Types/Medicare-Surety-Bond.asp

[13] http://innovation.cms.gov/initiatives/ACO/index.html

[14] http://medicaiddirectors.org/sites/medicaiddirectors.org/files/public/namd_cms_pi_efforts_121005.pdf

[15] http://www.whitehouse.gov/the-press-office/presidential-memorandum-enhancing-payment-accuracy-through-a-do-not-pay-list

[16] http://downloads.cms.gov/cmsgov/archived-downloads/SMDL/downloads/smd012098a.pdf

[17] https://oig.hhs.gov/oei/reports/oei-03-12-00070.pdf

[18] http://www.healthcare.gov/news/factsheets/2011/03/fraud03152011a.html

[19] http://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/downloads/highlights.pdf)

[20] http://www.justice.gov/usao/eousa/ole/mii/mii.fact.sheet.html

FRED UPTON, MICHIGAN
CHAIRMAN

HENRY A. WAXMAN, CALIFORNIA
RANKING MEMBER

ONE HUNDRED TWELFTH CONGRESS

**Congress of the United States**

**House of Representatives**

COMMITTEE ON ENERGY AND COMMERCE
2125 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6115

Majority (202) 225-2927
Minority (202) 225-3641

January 10, 2013

Ms. Alanna M. Lavelle, AHFI, MS, CPC
Director, Special Investigations
WellPoint, Inc.
120 Monument Circle
Indianapolis, IN 46204

Dear Ms. Lavelle:

Thank you for appearing at the Subcommittee on Health hearing entitled "Examining Options to Combat Health Care Waste, Fraud and Abuse."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for 10 business days to permit Members to submit additional questions to witnesses, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please e-mail your responses, in Word or PDF format, to carly.mcwilliams@mail.house.gov by the close of business on Thursday, January 24, 2013.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Joe Pitts

Joseph R. Pitts
Chairman
Subcommittee on Health

cc: Frank Pallone, Jr., Ranking Member, Subcommittee on Health

Attachment

**The Honorable Joseph R. Pitts**

1. **Your testimony references a recently contracted predictive modeling program, initially rolled out in Georgia, which will go company-wide in 2013; this modeling program allows WellPoint to review claims in both post-payment and pre-payment environments. How important to your program integrity efforts are systems designed to catch fraudulent claims before they are paid?**

   WellPoint has a responsibility to our customers to ensure that their health care dollars are used appropriately. Therefore, it is very important to WellPoint to focus on fraud prevention, since preventing fraud is more effective, and less expensive, than paying a fraudulent claim and trying to recoup those monies from a fraudulent entity, which may or may not be successful. Fraud prevention plays a critical role in reducing losses from fraud and abuse, as criminals commonly send monies offshore where they cannot be attached. In addition, equally important is ensuring patient safety by helping identify and remove providers and individuals who are engaging in unsafe and fraudulent practices from the health care system.

2. **Can you explain how predictive modeling helps WellPoint identify general weaknesses in its payment systems and procedures?**

   Our predictive modeling system uses six different analytics to analyze a year's worth of claims data to identify outliers and unusual patterns of claims submittal and payment, which we can then quickly address in order to determine if they may constitute fraud or abuse.

   An example where a predictive modeling system identified abusive practices is a case in which a provider was billing for fourteen units of urine drug testing per patient per day. After investigation of the matter we determined that the provider was improperly unbundling the claim. In fact, there was only one drug test performed each date, but it was for fourteen types of drugs. We have implemented processes in our systems to reduce the risk of future similar billing events. We anticipate a savings of $13M during 2013 as a result of these changes.

3. **You mention in your testimony that data sharing between public and private entities is very important for fraud prevention. Medicare Advantage seems like a good example of where public and private payers meet.**

   a. **What sorts of data sharing occur between Medicare and MA plan companies?**

   Medicare Advantage health plans hold a quarterly in-person meeting with the MEDICs (Medicare Drug Integrity Contractors) where data is shared between parties in order to identify possible improper or suspect activity by pharmacies, clinics, DME providers, etc. The MEDICs deal with both Medicare Parts C (Medicare Advantage) and D (the prescription drug plan).

   b. **Do you believe that data sharing could be improved between the two to improve fraud prevention? If so, how?**

   Once a MEDIC starts an investigation on a provider, it does not share information on the status of the case with health insurers until final adjudication. As result, the health plans may not know about developments in the investigation or information obtained for a number of years. This delay puts health insurers at a significant disadvantage because they cannot react to and prevent ongoing abusive behavior that a MEDIC may have uncovered. In many cases, health plans do not even get notice of sentencing and are required to use PACER, the federal court online records system, in order to determine whether a provider under a MEDIC investigation has been prosecuted.

Data sharing from HHS-OIG is even more limited. When HHS-OIG is prosecuting a provider for Medicare or Medicaid fraud, they tend not to focus on losses to Medicare Parts C and D, with even less attention paid to the losses of private health insurers. This lack of information sharing can result in significant improper payments that otherwise possibly could have been avoided.

One such case involves an HIV infusion scheme in Orlando, Florida. Patients received kickbacks from providers for letting the provider use the patient's health insurance ID to fraudulently bill plans. WellPoint identified the provider and then brought information to the FBI in order to address the situation collaboratively. During the course of the federal investigation, the provider continued to engage in the improper billing and WellPoint sustained a $12M loss on twelve members over a two year period. Before the government investigation could be completed, the provider sent the funds to an offshore account where they could not be attached

4. **As you know, the proponents of the MLR rule claim they are trying to cap the percentage of premiums that go to CEO salaries and profits, but I am greatly concerned that is not what this rule does. My fear is the rule will penalize plans that take steps to reduce costs and increase quality by designating good activities as 'administrative costs". Last year HHS Inspector General Daniel Levinson testified at this Subcommittee that health care fraud schemes commonly includes billing for services that were not provided or were not medically necessary, purposely billing for a higher level of service than were provided, misreporting costs or other data to increase payments, paying kickbacks, and/or stealing providers or beneficiaries identities. Given that all of these activities add unnecessary cost to the health system and if rampant would significantly increase premiums, do you believe that the MLR would increase consumer premiums or health care costs and how?**

   We agree that the MLR rule penalizes health insurers that sponsor robust anti-fraud programs by requiring that the majority of expenses for those programs be considered as administrative expense in the MLR calculation. Private health plans have known for decades that it is more efficient and less costly to prevent a fraudulent payment from occurring than to pay a fraudulent claim and have to recoup it, as recouping fraudulent payments is a long and costly process with no assurance that an insurer will be made whole. Fraud prevention can also help the entire health insurance industry as health insurers share information on fraudulent providers. Fraud prevention programs of health insurers can also assist the Medicare, Medicaid, and SCHIP programs by sharing fraudulent provider information with those government entities for criminal prosecution to remove the provider from the system entirely.

5. **If a health plan paid for upfront costs to implement systems to avoid paying fraudulent claims that would be counted as an administrative cost?**

   Yes. Examples of this include our unit that flags and reviews suspect providers' claims for fraud and abuse before they are paid, and our predictive modeling system which, as mentioned above, pinpoints unusual claims patterns and practices that can indicate fraudulent or abusive billing practices.

6. **Under the MLR rule is it considered an administrative cost if you try to recoup payment for a service the plan had paid for but was never provided? How would a cost be designated if the plan used procedures to ensure upfront they never pay for services that were not provided?**

   Yes, the cost of attempting to recoup improper payments would be considered administrative expenses, and the cost of preventive fraud programs are also considered administrative expenses. Insurers are very limited in the credit they receive in the MLR calculation for the expenses associated with their anti-fraud programs. In general, insurers are only granted credit for the expenses of anti-fraud programs for those monies that have been recouped. Thus, most of the actual costs of anti-fraud programs that are required on the front end in order to prevent fraud or to recoup improper payments must be allocated towards insurers' administrative expenses in the annual MLR calculation. The credit provided perversely encourages insurers to "pay and chase" rather than to prevent fraud and abuse.

7. **CMS announced in 2010 that it wanted to start requiring background checks on providers. To me that is a sensible anti-fraud tool. Under the medical loss ratio, would doing background checks and credentialing of providers be considered an administrative cost? Would this discourage this type of anti-fraud measure?**

   Health insurers' costs for provider credentialing are expressly considered to be administrative expenses for purposes of the MLR calculation. As health insurers are expected to absorb more and more administrative expenses, their ability to perform provider credentialing may be hampered.

8. **Bogus providers – those who possess National Provider Identifier Number but do not actually perform services – are a real threat to both commercial insurance and the Medicare program. From your experience, can you tell us how big this problem is?**

   We believe that the issue of bogus providers constitutes approximately a $100M problem, based on the experience of WellPoint and another large commercial carrier in 2010. WellPoint has felt the direct impact of bogus providers, particularly in the Medicare Advantage program. We are aware of over two hundred DME providers alone that are bogus.

   The typical scheme is for criminals to steal a provider's National Provider Identifier number, a task made easier because many providers do not protect their NPI as they would their Social Security Number or other confidential information. Criminals advertise on Craigslist to hire locum tenens providers, and when providers send in their CVs, most of the time their NPIs are listed on the resume. We have seen the bogus provider movement move from Florida to Georgia to Louisiana to Texas. Criminals will often conduct a "hit and run" on insurers and garner amounts up to and in excess of $1M of ill-gotten gains in a month, close up shop and then send the money offshore where it cannot be attached.

   WellPoint has taken proactive steps to try and identify these bogus providers, by comparing providers' P.O. Box numbers and NPIs to our database, which sometimes shows that one bogus provider merely switches names but uses the same P.O. Box or NPI to collect claims payments.

9. **We understand that a WellPoint subsidiary is part of the CMS predictive modeling program. Please explain the company's role in the program and give a status update on implementation. Does WellPoint have ideas on steps that could improve the program?**

   I am referring this question to National Government Services, WellPoint's subsidiary, to respond to this question, as NGS serves as the subcontractor to the CMS program.

   National Government Services response:

   National Government Services, a WellPoint subsidiary, serves in the role of subcontractor to Northrop Grumman Corporation on the CMS Enterprise System Developer Task Order "Predictive Modeling for the National Fraud Prevention Program." National Government Services, in its role as a subcontractor, provides hosting services, domain Medicare expertise, biostatisticians, user support, and development resources. The Fraud Prevention System, as it is commonly referred to, was operationalized and went live on June 30, 2011. We believe that by launching the Fraud Prevention System, the CMS has taken important steps towards the identification and prevention of Medicare fraud including their initiative to integrate the prevention program into the CMS shared systems, which will support the denial of fraudulent claims prior to payment adjudication. To further improve the overall system, we believe that as the program matures there is a great opportunity for further integration with additional data sources such as Medicaid and Part D, which will enhance the overall view and understanding that the CMS has into the systemic fraud challenges plaguing our healthcare delivery system.

10. **Can you please provide to the committee a list of the fraud prevention areas that WellPoint believes could be improved within CMS? If these areas include deficiencies on the part of CMS, please provide explanation as to why you believe those deficiencies exist. Can you also provide recommendations on ways that CMS fraud prevention can be improved?**

On June 29, 2012, WellPoint provided substantial comments to the Senate Finance Committee with recommendations on how CMS fraud prevention and investigations could be improved. Our recommendations included the following:

- **Move to Predominantly Prepayment Fraud Investigation in Medicare**

  Changing from primarily "pay and chase" fraud investigation to more of a "prepayment" fraud investigation style would have the largest immediate impact in the Medicare program. Indeed, the GAO has continued to recommend that HHS needs to fully implement prepayment fraud and abuse investigations to address fraud and abuse.[1] For example, WellPoint conducted a Medicare Part C investigation where a provider was billing the program for an infusion medication for HIV patients using a certain J-Code which reflected that the claim was for the "long lasting" medication, while actually injecting the regular medication. The long lasting medication is a once-a-month medication whereas the drug the provider was actually injecting is administered 3 times a week. As a result, WellPoint paid this particular provider $12M before data mining identified his claims as an outlier. Once his figures were reviewed for just 12 Medicare beneficiaries, the provider's claims were pended, which prevented another $2.5M from being issued to this provider. Had a pre-payment review been available, the review would likely have detected the medication actually billed for and caught the disparity with the frequency in which the provider was injecting it. This provider is currently being investigated by HHS-OIG.

  While CMS is examining DME reimbursement on a prepayment basis, it is clear that more of this needs to be done, including more collaboration between the administrative side of Medicare that pays claims and the Centers for Program Integrity (CPI) at CMS that investigates fraud. Currently Medicare Administrative Contractors (MACs) can often spot potential provider fraud being committed and have the ability to temporarily pend claims and/or refer their suspicions of fraud to CPI and DOJ. However, typically fraudulent claims will then continue to be paid while a criminal case is being built, which can often take months, if not years. While WellPoint understands the need to build a case for prosecution of committing fraud against the Medicare program, ***we believe that there needs to be a better balance between fraud prevention and paying claims. If MACs had the ability to stop making payments for claims once a certain evidentiary threshold for fraud or abuse has been reached, then fewer taxpayer dollars would be spent on improper Medicare payments.*** WellPoint recommends that there be collaboration between fraud and abuse investigatory experts at the CPI and the Department of Justice to establish clear policy guidelines to determine when sufficient evidence of fraud or abuse has been gathered to enable suspending claims payments.

[1] See GAO, *Medicare: Important Steps Have Been Taken, but More Could Be Done To Deter Fraud,* GAO-12-671T, and GAO, *Medicare Fraud Prevention, CMS Has Implemented a Predictive Analytics System, but Needs to Define Measures to Determine Its Effectiveness,* GAO-13-104.

- **Broaden Efforts to Capture Improper Payments**

  We know that upcoding, unbundling, and other types of "code creep" occur relatively frequently in provider billings to private health insurance plans. Predictive modeling suggests that it is also likely that improper coding occurs in the Medicare fee for service program as well. CMS should focus some resources on investigating abusive "code creep" and administer appropriate reduced payments.

- **MEDIC Feedback to Plans on Result of Fraud Referrals**

  MEDICs operate outside of the data systems at CMS and, as we indicated above, do not share information about fraud investigations they may be pursuing. When insurers submit fraud referrals to the MEDICs, MEDICs rarely provide any feedback to plans on the results of the fraud referral. We recommend that the MEDICs report back to plans on the results of their fraud referrals.

- **Extend Medicare Fraud Prevention Systems and Procedures to Medicaid**

  Currently states are putting out RFPs to license fraud investigation systems, with no coordination between the states. Purchase of 50 different sets of software solutions seems needlessly duplicative and costly to the states and will likely cause barriers to efficient and effective fraud investigation.

  We recommend that CMS leverage the investments it has already made in this area to share with the states the same tool that Medicare is using. CMS has already indicated that it is evaluating the use of its Medicare Fraud Prevention System (FPS) and Automated Provider Screening (APS) on state Medicaid data.[2] CMS is planning several pilot programs to analyze one state's data using the FPS, as well as screening all of one state's Medicaid providers using the APS. We applaud these efforts and encourage CMS' planned expansion of the FPS and APS to other states as well.

- **Implement Medicare Restricted Recipient Program**

  WellPoint supports giving CMS the authority to establish a restricted recipient program in Part D for those beneficiaries displaying a pattern of misutilization, as this is a practice that health plans have adopted for other lines of business. We also recommend that insurance organizations sponsoring Part D plans ("plan sponsors") be permitted to report beneficiary-specific concerns—based on objective, standardized metrics—to CMS or to the MEDICs for appropriate action against the individual beneficiary. To ensure members' safety, WellPoint believes that plans should not implement policies of denying a prescription fill even in cases of suspected overutilization. Rather, we believe the plan sponsor should identify cases of suspected misuse or overutilization of prescription medications and turn over detailed information to CMS, which would then be responsible for taking any enforcement action once further investigation has taken place.

[2] Statement of Peter Budetti, M.D., J.D., Deputy Administrator and Director, Center for Program Integrity, Centers for Medicare & Medicaid Services, on "Saving Taxpayer Dollars by Curbing Waste and Fraud in Medicaid," before the U.S. Senate Committee on Homeland Security and Government Affairs, Subcommittee on Federal Financial Management, Government Information, Federal services and International Security, June 14, 2012 (found at: http://www.hsgac.senate.gov/subcommittees/federal-financial-management/hearings/saving-taxpayer-dollars-by-curbing-waste-and-fraud-in-medicaid [last visited 6/20/12]).

Furthermore, WellPoint supports flexibility for MA and PDP plans in their implementation of fraud and abuse detection processes. We note that one model will not work for all plan types; for instance, stand-alone PDPs will need to deploy processes differently from coordinated care MA-PD plans. Rather than articulating detailed protocols in statute or regulation, we suggest that plans be permitted to file a program description subject to certain articulated parameters, which could be approved or denied by CMS.

- **Lock Dual Eligibles with Drug Seeking Behavior into One Managed Care Plan**

Through our experience in providing health care coverage through both our Medicaid state-sponsored programs and Federal programs, we have observed that a large portion of the opioid and controlled substance abuses in the Part D program occur among the dual eligible population – beneficiaries eligible for both Medicare and Medicaid and often under 65 years of age. In calendar year 2012 alone, WellPoint's SIU unit tracked 43 investigations of Medicare Part D beneficiaries under the age of 65. Under current law, dual-eligible beneficiaries are allowed to change plans on a month to month basis, which permits drug seekers to switch programs frequently in order to avoid detection and escape program edits or substance abuse programs.

WellPoint recommends that dually eligible beneficiaries with evidence of drug-seeking behavior should be locked into one managed care plan, rather than continue to be allowed to switch plans on a monthly basis to evade detection.

- **Improve Fraud-Fighting Partnerships Between Plan Sponsors and Government**

WellPoint supports better coordination and cooperation among CMS, DOJ, and all stakeholders. WellPoint supports the development of a plan by all stakeholders, and stresses that plan sponsors should be included in the development of such a plan. Right now there is little collaboration between the agencies and the health plans that oftentimes have the information, experience and expertise necessary for preventing and fighting fraud and abuse. While health plans currently share information with the MEDIC, we are rarely informed of the ultimate result, and information collected by the agency is rarely shared with our fraud and abuse detection teams. As we have stated many times, only an effective partnership between private and public health care programs can effectively reduce the incidence of fraud and abuse. We are optimistic about the recent creation of the Healthcare Fraud Prevention Partnership, and are hopeful that through the work of the Partnership there will be real progress towards successful public/private collaboration in the prevention and detection of health care fraud and abuse.

However, WellPoint is concerned that any requirements for health plans to share data with other plans regarding the record and actions generated by overutilization review -- for example, the record from the retrospective drug utilization review (DUR)/case management, as well as beneficiary-specific point of service (POS) edits -- could have negative unintended consequences. As a threshold matter, this type of data sharing will be administratively burdensome for plan sponsors and may also have negative unintended consequences for the beneficiary. For instance, if a beneficiary changed plans because he felt he was being unjustly targeted by his prior plan when in fact he had an underlying medical condition that warranted his drug utilization, the beneficiary may face continued barriers to obtain needed treatment if the new plan is bound by information provided by the prior plan.

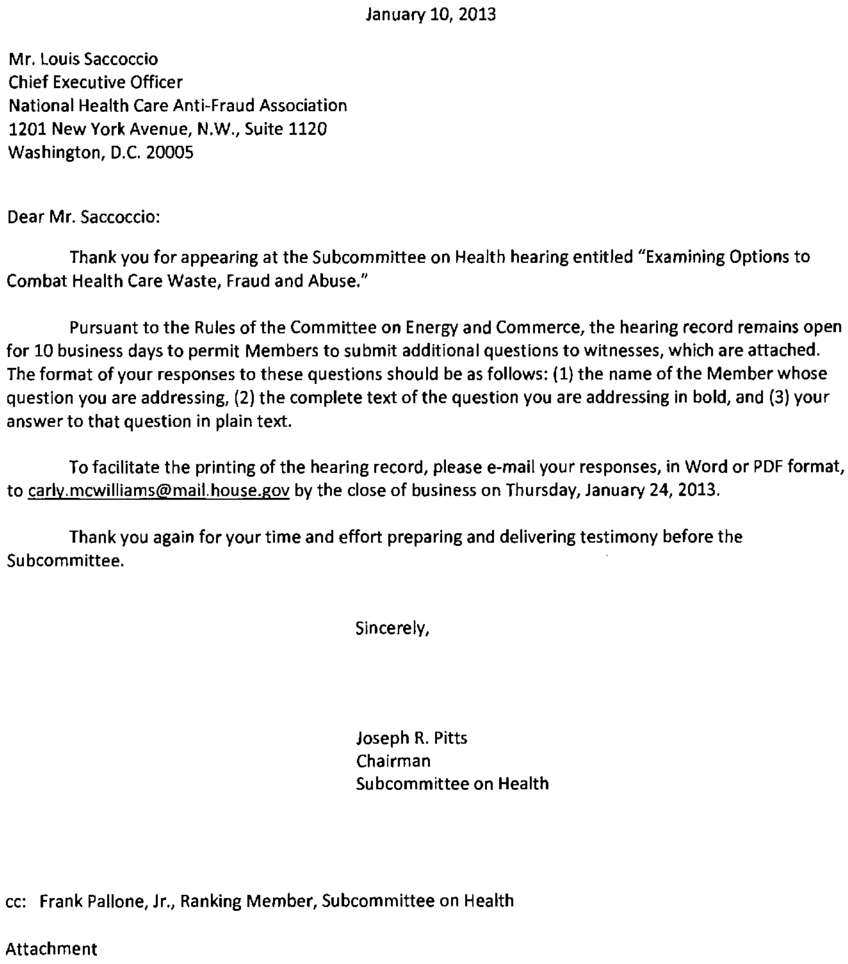
Instead, each plan sponsor should be encouraged to put its own practices in place to appropriately screen new members, rather than being required to act on information that they do not have firsthand, verifiable evidence to support. Each health plan should then convey any information regarding suspected fraud or abuse to CMS and the MEDICs. WellPoint recommends that CMS and the MEDICs have responsibility for maintaining this information and sharing it with appropriate agencies and plan sponsors, such as when a suspected member switches from one health plan to another. WellPoint also recommends extending the application of data-sharing efforts to providers identified as potentially fraudulent.

- **Expand Medical Loss Ratio Credit for Private Plans' Fraud Prevention Efforts (Including for Medicare Advantage)**

In order to alleviate the time, effort and expense required for the greater detection and curtailing of fraud and abuse in the health care system, such expenses should not be accounted for as administrative expenses under the MLR calculation, but rather be included under "activities that improve health care quality." These activities enhance patient safety by helping to remove from the system health care providers and individuals engaging in unsafe and fraudulent practices. They also can help guide beneficiaries involved in substance abuse to appropriate treatment programs and enforce appropriate drug protocols.

Just one example of how anti-fraud activities enhance patient safety is when patients engage in "doctor shopping" at emergency rooms to receive multiple prescriptions for opioid or other Schedule II medications. These patients will oftentimes undergo multiple imaging (CTs or X-rays) on a weekend, exposing them to far too much radiation. Intervention by anti-fraud investigators can not only put a stop to inappropriate prescribing, but protect patients from too-frequent doses of radiation as well.

The MLR regulations merely give insurers a limited credit – up to the amount of fraud recoveries – for fraud prevention activities. In essence, this means that insurers will have to count as administrative expenses their largest portion of anti-fraud expenses -- those dedicated to fraud prevention. It is truly puzzling that at a time when the federal government is accelerating its efforts to prevent fraud in Medicare and Medicaid, it has simultaneously issued a regulation that will serve to discourage health insurers' fraud prevention efforts. Ironically, eliminating anti-fraud programs will tend to increase MLR percentages because claims will be higher, but an increased MLR will be at the expense of patient safety, quality of care, and controlling health care costs, which are the very aims of the Affordable Care Act. If private health insurers are discouraged from keeping their anti-fraud programs in place at the same time that public program anti-fraud efforts are increasing, federal law enforcement will lose a valuable source of information and tips about providers and recipients who may also be engaging in defrauding public programs. These considerations will also be crucial as the CMS codifies and implements the ACA's MLR for Medicare Advantage.



January 10, 2013

Mr. Louis Saccoccio
Chief Executive Officer
National Health Care Anti-Fraud Association
1201 New York Avenue, N.W., Suite 1120
Washington, D.C. 20005

Dear Mr. Saccoccio:

Thank you for appearing at the Subcommittee on Health hearing entitled "Examining Options to Combat Health Care Waste, Fraud and Abuse."

Pursuant to the Rules of the Committee on Energy and Commerce, the hearing record remains open for 10 business days to permit Members to submit additional questions to witnesses, which are attached. The format of your responses to these questions should be as follows: (1) the name of the Member whose question you are addressing, (2) the complete text of the question you are addressing in bold, and (3) your answer to that question in plain text.

To facilitate the printing of the hearing record, please e-mail your responses, in Word or PDF format, to carly.mcwilliams@mail.house.gov by the close of business on Thursday, January 24, 2013.

Thank you again for your time and effort preparing and delivering testimony before the Subcommittee.

Sincerely,

Joseph R. Pitts
Chairman
Subcommittee on Health

cc: Frank Pallone, Jr., Ranking Member, Subcommittee on Health

Attachment

**The Honorable Joseph R. Pitts**

1. You mentioned in your testimony the resulting instances of patient harm that arise from Medicare fraud – can you provide some examples?

   Patient harm arising from health care fraud is unfortunately commonplace. Cases involving Medicare recipients—comprised mainly of our nation's vulnerable, senior population—are particularly prevalent. Patient harm can come in many forms.

   A common type of case is one in which a patient is subjected to medical services or procedures, some of which may be invasive and dangerous, that are not medically warranted and are provided or performed solely for the purpose of generating claims for payment. In addition to being subjected to an unnecessary medical procedure, the patient must deal with the concern and anxiety that accompanies such procedures. Concurrently, the patient's medical record and history present a false picture of the patient's health and condition going forward as a result of this type of scheme.

   Other cases of patient harm can arise from pharmacy fraud where prescription drugs may be shorted or diluted when provided to the patient. There are even cases where patients have been provided placebo-type drugs instead of the necessary drugs they were supposed to receive for their conditions. Additionally, seniors can be the victims of abuse and neglect at nursing homes.

   The following are cases that provide real life examples of patient harm. These cases are summarized in the two most recent annual reports to Congress from the Department of Justice and the Department of Health and Human Services under the Health Care Fraud and Abuse Control (HCFAC) Program:

   *"In June 2011, the U.S. District Court in Miami sentenced a physician to 235 months in prison for his role in a $23 million injection and HIV infusion scheme. The physician[...]* ***diagnosed almost all patients with the same rare blood disorders, which the patients did not have, and prescribed expensive medications to the patients for the sole purpose of receiving Medicare reimbursements. The court also found that the physician obstructed justice by testifying falsely at his trial, and that he caused a risk of serious bodily injury to his patients."*** –pg 12, HCFAC Program, Annual Report for Fiscal Year 2011

   *"In December 2010, the owner and operator of a medical clinic in Miami was sentenced to 60 months in prison for his role in a $16.6 million Medicare fraud scheme.[...] The clinic allegedly* ***provided unnecessary prescriptions, plans of care and medical certifications to Miami-area home health agencies in return for kickbacks and bribes,*** *and falsified patient files to make it appear as if Medicare beneficiaries qualified for daily skilled nursing visits."* –pg 12, HCFAC Program, Annual Report for Fiscal Year 2011

   *"In June 2011, the co-owner of two Michigan nerve conduction clinics was sentenced to 15 months incarceration for her role in a Medicare fraud scheme. Between September 2007 and June 2008, the individual and co-conspirators used the clinics to bill Medicare for unnecessary tests and services, including nerve conduction studies. [...]* ***the patients received $50 to $75 in exchange for subjecting themselves to the medically unnecessary tests."*** – pg 16, HCFAC Program Annual Report for Fiscal Year 2011

   *"In June 2011, prosecutors filed an indictment charging a Chicago man who operated two home health care businesses[...]* ***The defendant, who had no formal medical training, medical degrees, or licenses to practice as a health care professional, allegedly schemed with others to submit millions of dollars in false claims for reimbursement of home health care services***

***purportedly provided to Medicare beneficiaries, which allegedly were never provided, were not medically necessary..."*** –pg 20, HCFAC Program Annual Report for Fiscal Year 2011

*"In December 2010, o Grand Rapids dermatologist wos sentenced to 120 months in prison following his jury conviction on 31 counts of health core froud.[...] The evidence ot sentencing included expert testimony that* ***many patients had undergane unnecessary surgical procedures to have benign skin lesions removed in order to fuel the dermatologist's various fraud schemes. The investigotion and prosecution also revealed that the dermatologist had reused sutures on multiple patients, resulting in the notification and testing of thousands of patients for HIV and Hepatitis C by the county health department."*** –pg 26, HCFAC Program Annual Report for Fiscal Year 2011

*"In September 2010, a formerly licensed nurse in Puerto Rico wos sentenced to 18 months of incarceration after pleading guilty to four counts of misbranding of a drug with the intent to defraud.* ***Though not licensed as a physician, this individual presented himself as a physician specializing in wound care, treated several beneficiaries suffering from skin ulcers, and regularly provided patients with prescriptions for medications to treat such conditions."*** –pg 26, HCFAC Program Annual Report for Fiscal Year 2011

*"In October 2009, the court sentenced a defendant who falsely claimed to be a physician's assistant and who worked for two separate Miami-area HIV-infusion clinics to 108 months of imprisonment.[...] Over a two-year period,* ***the clinics submitted more than $12 million in false claims to Medicare for expensive HIV-infusion therapies when, in fact, they were providing the patients with nothing more than injections or infusions of Vitamins B-6 and B-12."*** –pg 12, HCFAC Program Annual Report for Fiscal Year 2010

*"In August 2010, the court sentenced a Miami resident who was an operator of a Detroit-orea medical clinic to 56 months in prison for his role in a $2.2 million scheme to bill Medicore...* ***The Medicare beneficiaries who received the kickback payments also agreed to feign certain symptoms and subject themselves to medically unnecessary diagnostic tests and examinations which led to the patients' medical records to contain information about false symptoms."*** –pg 14, HCFAC Program Annual Report for Fiscal Year 2010

*"In December 2009, a Virginia mon was sentenced in the District of Columbia to 13 months in prison followed by three years of supervised release for impersonating a doctor.[...]* ***The defendant pretended that he was a doctor and prescribed medicine by using the identities of four different victim doctors. In truth, the defendant was never a licensed medical doctor and was not authorized to practice medicine.[...] Over the course of the scheme, more than 200 patients saw the defendant and believed him to be a licensed medical doctor capable and authorized to treat mental health illnesses."*** –pg 26, HCFAC Program Annual Report for Fiscal Year 2010

*"In April 2010, a Pennsylvania pharmacist was sentenced to 18 months in prison and ordered to pay $576,000 in restitution after pleading guilty to charges of drug adulteration and misbranding, health care fraud, mail froud, and aiding and abetting. [...]* ***The investigation also reveoled that the pharmacist's compounded drugs were contaminated with bacteria, and that he manufactured the compounded drugs without using medicinal quality water, weoring gloves, or wearing a mask. Additionally, in making o budesonide-based drug intended for asthma patients, he used chemicals such as ethyl alcohol and Everclear (a pure grain alcohol), which are severe irritants to the respiratory system."*** –pg 28, HCFAC Program Annual Report for Fiscal Year 2010

> *"In January 2010, five nursing homes operated by Cathedral Rock, a Texas corporation, pled guilty to felony health care fraud related to the failure to provide adequate care to the Medicare and Medicaid residents living in those homes.[...]* ***the nursing homes admitted that, at times, their staffing was insufficient to provide adequate nursing care or to provide wound care; that residents often did not receive their medication as prescribed; that medical records were falsified and a "charting party" occurred to fill in medical records so that it appeared that all medication had been properly given, regardless of whether the medication was actually given or not;*** *"* –pg 30, HCFAC Program Annual Report for Fiscal Year 2010

The following are links to a few recent news stories that also illustrate patient harm fraud cases involving Medicare patients:

For-Profit Nursing Homes Lead in Overcharging While Care Suffers, Bloomberg, December 31, 2012, http://www.bloomberg.com/news/2012-12-31/for-profit-nursing-homes-lead-in-overcharging-while-care-suffers.html

Medicare fraud nets 10-year prison term for Palos Hills man, SouthtownStar, December 20, 2012, http://southtownstar.suntimes.com/news/17143092-418/medicare-fraud-nets-10-year-prison-term-for-palos-hills-man.html

Doctor Accused of Diluting Chemo, Bilking Medicare Pleads Guilty, LymphomaInfo.net, July 18, 2012, http://www.lymphomainfo.net/news/cancer/doctor-accused-of-diluting-chemo-bilking-medicare-pleads-guilty

Medicare Records Reveal Troubling Trail of Surgeries, Wall Street Journal, March 29, 2011, http://online.wsj.com/article/SB10001424052748703858404576214642193925996.html

2. As you state in your testimony, The Office of National Drug Policy calls prescription drug abuse "the Nation's fastest growing drug problem" and the Centers for Disease Control and Prevention classifies drug abuse as an epidemic. This epidemic fueled the practice of doctor shopping and is a large source of fraud in private health insurance plans. Do you have any sense of how prescription drug abuse and doctor shopping impacts the Medicare program? Do you believe that some of the solutions for this problem being undertaken by private payers would work in Medicare?

   To gauge how prescription drug abuse and doctor shopping impact the Medicare program, NHCAA depends largely on two Government Accountability Office (GAO) reports issued in the fall of 2011 that examine this very problem:

   - "MEDICARE PART D: Instances of Questionable Access to Prescription Drugs" October 4, 2011, http://www.gao.gov/assets/590/585579.pdf
   - "MEDICARE PART D: Instances of Questionable Access to Prescription Drugs" September 2011 http://www.gao.gov/assets/590/585424.pdf

   These reports certainly indicate that Part D is vulnerable to prescription drug abuse.

   This we know: prescription drug fraud is a serious issue with severe patient harm risks. Overdoses resulting from the abuse of prescription drugs are sadly commonplace, and in many cases the drugs taken were obtained by filing false claims. Moreover, not only do government programs and private health insurers pay for the unnecessary prescription drugs, they also pay for the related medical services (e.g. emergency room services) provided to the patient which may have been feigned in order to obtain the prescriptions.

Private health insurers continue to devote increased attention and resources to prescription drug fraud, devising new and innovative ways to detect possible drug diversion and doctor shopping and then taking appropriate steps to stop it, while also trying to help patients in need of intervention and treatment.

Some state Medicaid programs and private health insurers have implemented innovative programs that CMS may want to consider adopting for the Part D program. These include:

- The use of overutilization reports;
- Letter campaigns making prescribers aware of possible drug-seeking behavior;
- The implementation of restricted recipient or "lock-in" programs whereby the patient is limited to filling prescriptions at one pharmacy. (A lock-in program could also require a patient to receive prescriptions from just one doctor.)

To anyone who remains skeptical that prescription drug abuse is truly a serious problem, we offer the following case, which describes a health care fraud investigation significant enough to be named as NHCAA's Investigation of the Year for 2010.

In October 2010, a Kansas physician named Stephen J. Schneider and his wife, Linda K. Schneider, a licensed practical nurse who also acted as the office manager of her husband's pain management clinic, were sentenced to 30 and 33 years in federal prison, respectively, for illegally distributing prescription pain medication to patients who overdosed. A four-year investigation of this "pill mill" uncovered evidence of extensive over-prescribing of controlled substances by Dr. Schneider.

More than 100 drug overdoses requiring visits to Wichita-area emergency rooms and the deaths of at least 68 persons are linked to this case, as well as more than $4 million in Medicaid and private insurance claims. A 34-count indictment charged the Schneiders with health care fraud resulting in death, unlawfully dispensing controlled substances resulting in death, conspiracy, submitting false claims and money laundering. After an eight-week trial, the jury convicted Stephen Schneider on 19 counts and Linda Schneider on 32 counts, finding that the couple directly contributed to the deaths of several patients. Presiding U.S. District Judge Monti L. Belot offered a bleak and succinct summary of the case calling it "an avoidable tragedy motivated by greed."

3. In your opinion, what are the new and emerging health care fraud areas that we should be concerned about in Medicare?

Fraud trends and schemes are constantly changing, developing, and migrating from one area of the country to another. Those seeking to commit health care fraud are opportunistic by nature and will seek out weaknesses wherever they exist.

The below listed areas are those which the experience of our members and current trends indicate to be most susceptible to fraud. Many of these areas are not new to the list:

- Organized criminal enterprises (could invoke several types of schemes but seem to depend significantly on medical identify theft—theft of patient and provider identities)
- Pharmaceutical/Drug Diversion
- Home Health Care
- Infusion Therapy
- Pain Management (office-based opioid therapy (OBOT))

- Durable Medical Equipment (involves significant medical identity theft)
- Behavioral health and community mental health centers
- Medical Identity Theft (Medical ID theft is often an element of a broader health care fraud scheme)
- Cardiology
- Ophthalmology
- Physical therapy and occupational therapy (medical necessity, spa vacations)
- Transportation (ambulatory)

4. In your testimony, you mention the importance of data sharing in support of anti-fraud tools and how the Healthcare Fraud Prevention and Private Partnership announced in July of this year will help facilitate such data sharing. To date, how many meetings have been held?

   After more than two years of thoughtful discussion and collaboration among several interested parties, the Healthcare Fraud Prevention Partnership (HFPP) was formally announced at the White House in July, 2012. The primary goal of the HFPP is to foster more effective information sharing between the public and private sectors as a means to fight health care fraud.

   Significant consideration was given to establishing a sustainable framework for the HFPP. It includes an Executive Board as well as two committees where the information sharing work takes place:

   - The Data Analysis and Review Committee (DARC)
   - The Information Sharing Committee (ISC)

   In addition, the project's structure allows for "Participating Entities" which are organizations that have medical claims payment or other data that they wish to share with the HFPP in order to combat health care fraud. NHCAA is represented on the Executive Board as well as both committees.

   The Executive Board held its first meeting on September 19, 2012, and will meet again this year as necessary depending on the work coming from the two committees. The DARC and the ISC have held numerous meetings and continue to meet. The DARC is working on several first-step initiatives through which specified data will be shared by private health plans and the government. The ISC is working on establishing a protocol for sharing the information derived from the work of the DARC among health care payers.

   NHCAA believes the HFPP has the potential to yield results that can significantly impact the fight against health care fraud.

5. Can you please provide to the committee a list of the fraud prevention areas that you believe could be improved within CMS? If these areas include deficiencies on the part of CMS, can you provide explanation as to why you believe those deficiencies exist? Can you also provide recommendations on ways that CMS fraud prevention can be improved?

   NHCAA believes that historically, CMS relied too greatly on a "pay and chase" model of fraud fighting. Too little attention was given to analyzing claims data for potential fraud before payment was made. However, we believe that CMS's shift in strategy to one which emphasizes prevention is the right one. The key to the success of this strategy will be the effective application of predictive analytics to Medicare claims. CMS has begun to apply predictive analytics with its Fraud Prevention System (FPS).

   CMS recently issued its first report to Congress on the FPS. NHCAA believes that as CMS becomes more proficient with the operation of the system and as more predictive models are developed and refined, the system will begin to have a significant impact on the both the detection and prevention of potential fraud.

Another major weakness in the Medicare program from an anti-fraud perspective has been the lack of effective screening of providers entering the system. Medicare fee-for-service (Parts A and B) is an "any willing provider" system which allows health care providers from across the nation to become Medicare providers upon acceptance of an application. This type of system is vulnerable to individuals and companies seeking to enter the system to commit fraud. However, this weakness is now being addressed to a large degree by CMS under the provisions of the Affordable Care Act and the regulations issued pursuant to the Act requiring enhanced screening of providers based on the risk the providers potentially pose for fraud. More effective screening is now being done, especially for those categories of providers which have traditionally been the source of significant fraud. CMS also has implemented an automated provider screening process which will assist in preventing individuals intent on committing fraud from entering the system.

As with most things, success is often linked closely to the level of resources devoted to the task. In recent years, increased emphasis has been given to the use of technology, including predictive modeling and prepayment analytics. This is necessary and important. However it is also vitally important to ensure that a trained and plentiful investigative workforce is in place so that we can make the most of these new technology tools now available to us.

Finally, NHCAA encourages CMS to continue to make cooperation with the private sector a priority. Investigative information sharing is a reoccurring theme in every discussion we have about how best to combat health care fraud. We believe that government entities, tasked with fighting fraud and safeguarding our health system, and private insurers, responsible for protecting their beneficiaries and customers, can and should work cooperatively on this critical issue of mutual interest. Our experience has taught us that investigative information sharing is a highly effective tool in combating health care fraud.

The Healthcare Fraud Prevention Partnership (HFPP) is a promising venue where CMS can demonstrate its support of investigative information sharing against health care fraud. CMS has access to an immense amount of health care claims data which can be harnessed to extract anti-fraud information that can be shared with other payers, yielding results that include:

- More complete billing profiles of aberrant providers that show their activities across multiple payers;
- Identifying industry-wide (as well as migrating regional) patterns, trends and schemes;
- The use of compiled data to enhance predictive models and for additional data analysis.

*Questions for the Record responses respectfully submitted by:*

Louis Saccoccio
Chief Executive Officer
National Health Care Anti-Fraud Association
1201 New York Avenue NW
Suite 1120
Washington, DC 20005
Phone: 202.659.5955
January 2013

# Answers to Questions Posed by Members of the House Energy & Commerce Subcommittee on Health Regarding the Hearing Entitled "Examining Options to Combat Health Care Waste, Fraud and Abuse"

Submitted by
**Neville Pattinson**
Senior Vice President, Government Affairs
Standards and Business Development
Gemalto, Inc.

<u>**The Honorable Joseph R. Pitts**</u>

1. **In your testimony, you stated that a common access card "verifying and coding each (Medicare) transaction" might help solve some of integrity problems within Medicare caused by phantom billing and processing errors. Can you give me a sense of how that might work?**

Under the current Medicare system, there are multiple opportunities for both fraud and errors to occur. Some common problems include:

**Provider-Based Fraud and Error:**

- Phantom billing is where fraudsters or unscrupulous medical providers bill Medicare for unnecessary or unperformed procedures, medical tests, or equipment (or for equipment that is billed as new but is, in fact, used).

- National Provider Identity (NPI) numbers of upstanding providers are stolen by fraudsters and criminals and used to file claims. In this case providers are unaware their Medicare account is being used for nefarious purposes.

- Durable medical equipment abuse can happen when medical equipment used in the home - like wheelchairs or oxygen tanks - are billed many times over, while in fact nothing has been delivered to an actual patient.

- Processing errors and mistakes account, in many cases, for improper payment. These payments either should not have been made or were made in an incorrect amount. Improper payments also include payments sent to the wrong recipient or payments where supporting documentation is not available.

**Patient-Based Fraud:**

- Fraudulent patient billing can occur when a patient provides his or her Medicare number to a provider in exchange for kickbacks. The provider bills Medicare for any reason and the patient is told to admit that he or she indeed received the medical treatment.

- "Card Swapping" passed-off or stolen Medicare cards are used by others to get medical care.

A Medicare common access card (CAC) can help eliminate these problems, significantly reducing opportunities for fraud and error. A Medicare CAC would leverage the existing government Personal Identity Verification (PIV) platform for secure identity credentials to modernize how information is protected within the Medicare system itself. Doing so protects the personal information of every beneficiary and puts in place a front-end prevention system to only allow authorized providers and suppliers to bill for Medicare services.

Authenticating Medicare beneficiaries and providers during an enrollment process and requiring the use of secure personalized credentials will reduce fraud by:

- Verifying beneficiaries are authorized to receive services and pharmaceuticals or equipment being prescribed;

- Verifying providers are authorized to provide those services and bill Medicare;

- Verifying suppliers, such as durable medical equipment (DME) vendors, are authorized to provide products and/or services and bill Medicare

- Preventing imposters from posing as beneficiaries or providers, thereby thwarting fraudulent transactions; and

- Verifying and coding each transaction to prevent phantom billing, processing errors and DME abuse.

Today when a beneficiary first enrolls in the Medicare program they verify their identity with documents or certificates on record with the Social Security Administration. Under Medicare CAC the process for beneficiary enrollment would not change. After electing to receive Medicare, beneficiaries receive a new secure smart card in the mail containing their protected identification information on an embedded micro-controller. For security purposes, a unique PIN code would be mailed to the beneficiary separately. The card and PIN together authenticate the beneficiary at check-in and authorize the transaction with the provider at the point of service or check-out. This process, using a smart card with a PIN code, is known as two-factor authentication.

Medicare providers verify their identity and eligibility to provide services during an enrollment process. Currently, under the Affordable Card Act (ACA) high risk providers go through an enrollment process to verify their credentials and identity. Under the proposed Medicare CAC, each provider's identity is secured by supplying a biometric that will serve as their own unique key to their Medicare billing account. Providers receive a secure smart card which includes an embedded micro-processor that stores basic biographical information, their NPI, as well as their unique biometric key, thus binding the credential to the individual. The card and the biometric together authenticate the provider, similar to two keys used to open a safety deposit box (another type of two-factor authentication).

At the point of service, the transaction is authorized by both the provider and the beneficiary by creating an electronic verification between their two smart cards using the unique keys – in this case, the beneficiary's PIN code and the provider's biometric. This verification is critical as it creates a confirmation by both parties that the service was rendered. The two-factor authentication process (card plus PIN for beneficiaries and card plus biometric for providers) limits the ability of criminals to fraudulently bill Medicare by posing as a either a provider or beneficiary. It's important to note that this represents two major improvements over the current system: first, a successful transaction requires two parties, and second, each of those parties must provide two-factor authentication of their respective identities.

Unauthorized services and product transactions are essentially eliminated since both the secure smart card and the person who owns the key on the card are required to conduct the transaction. This means that phantom billing, fraudulent patient billing and stolen Medicare cards are no longer easy means of bilking Medicare. Furthermore, both parties to the intended transaction must verify the transaction. In addition to imposing strict anti-fraud mechanisms, a Medicare common access card would also reduce processing errors (duplicate or misdirected payments) through electronic verification of data and digitally signed electronic billing processes.

2. **Mr. Pattinson, please explain how a smart card would work in the Medicare environment and why you believe your industry would be able to save close to 50% of the fraud being committed today.**

The way Medicare CAC would work in the Medicare environment is not significantly different than how current transactions are conducted in the doctor's office. The only difference is that instead of the provider taking a photocopy of the beneficiary's Medicare card to be used later as a reference for billing to be done later in the day – as is common practice today – the beneficiary and the provider would simultaneously present their cards to an authorized Medicare CAC reader. The beneficiary's Social Security number (the current Medicare identifier) is never revealed to the provider, nor is it sent in the clear through the network. Instead, it is sent in an encrypted format to CMS that only the authorized system can read, along with a digitally signed electronic certificate authenticating the transaction and the participants. In a situation where the beneficiary is not in possession of their card at the moment of the transaction, or in making an online purchase of Medicare-covered goods or services, CMS can handle the transaction as they do now when the beneficiary does not have their card, as well as create new policy options.

The Secure ID Coalition estimates that the Medicare can save over 50% of the cost of fraud based on a number of past smart card implementations throughout the federal government, as well as the international financial services and health care systems. As the US health care market is begins adopting smart cards, it also is realizing benefits. Below are just a few examples of smart card deployments that have resulted in significant savings.

**The Federal Government**

In addition to helping reduce fraud costs around the world, smart cards have been a reliable resource throughout the federal government for identity management and security for more than a decade. Designed on open standards approved by NIST, smart cards use non-proprietary technologies to help secure American's identity and security both home and abroad. Most significantly, the Department of Defense (DoD) Common Access Card (CAC) has shown the true security value of the smart card in protecting against fraudulent transactions and unauthorized access. Today every federal agency, including the DoD, utilizes secure smart cards to authenticate and verify users for building and computer access. While it is hard to measure fraud within government agencies, the DoD confirms a 46% reduction in cybersecurity attacks on the first day of secured computer access implementation.

**Financial Services**

The smart card technology present in the proposed Medicare CAC Act has been used to great success across the globe to protect identity and secure transactions not only in health care, but in the financial services market as well. Known as "Chip & PIN," the smart card technology has revolutionized the way banks have reduced fraud and identity theft. As testimony to their security and efficacy in fighting fraud, American banks will be introducing Chip & PIN cards to the U.S. market beginning in 2013. Examples of success include:

- United Kingdom Chip & PIN smart card deployment for credit and debit card market. According to a UK Payments Administration reported in 2010, overall fraud losses in the UK fell by 67% and counterfeit card fraud losses have decreased by 77% since 2004, when Chip & PIN was adopted.

- France's Chip & PIN smart card deployment for credit and debit card market. The French banking association GIE CB reported in November 2010 that a fraud ratio of 0.072%, for a total 350 million (USD) – of which $140 million (USD) originated outside France. Five years ago 26% of the system wide fraud was attributed to the Internet and 74% attributed to the real world. Today the numbers are exactly the opposite with 75% attributed to Internet fraud and 25% to real world. GIE CB credits smart cards with reducing real world fraud. For a frame of reference, over 3.5 billion smart card transactions occur every year for a value of $597 billion (USD). There are 58 million smart banking cards in circulation in France (population 64m) with an average of 113 operations/transactions per user.

**International Healthcare**

A number of nations have implemented smart card-based healthcare systems for many reasons beyond fraud reduction, such as security and ensuring administrative cost savings.

- French healthcare system SESAM-Vitale. The French government implemented smart cards in order to verify who was receiving treatment and to quickly provide reimbursements within three to five days as opposed to 3-4 weeks. As a result, the processing cost of a claim within the system was reduced from 1.74 Euros to .27 Euros. With over one billion transactions per year, the transition saves the system over 1.4 billion Euros/year.

- German Ministry of Health. Germany deployed secure smart healthcare cards to approximately 70 million beneficiaries and is currently deploying about 280 thousand health professional cards. The projected achievable program savings in the German national program range from 1.7 to 2.9 billion Euros per year, of which between 800 million to two billion Euros would come from fraud reduction. According to the German Ministry of Health in January 2012, the beneficiary deployment alone has generated annual fraud reduction of 250 million Euros. Provider fraud reduction data will not be available until deployment is completed next year.

- Taiwan. The Taiwanese government implemented one of the longest standing and most comprehensive secure health care cards in the world. Implemented in 2004, the program has issued 24 million patient cards and 300 thousand provider cards. The card data includes not only insurance information but medical information as well. The Bureau of National Health in Taiwan reports that moving from paper to a secure smart card has extended the life of cards by 5-7 years, reduced fraud, saved on administrative costs, and reduced health care spending in general. Taiwan's administrative costs are the lowest in the world at two percent (compared to the U.S. at 31 percent).

**US Healthcare**

While there are myriad examples of smart card implementations in healthcare across the US, we've chosen to highlight two showing cost savings for both large and small hospitals alike.

- Mt. Sinai Hospital, New York City. When Mt. Sinai deployed smart cards to their patients to reduce the number of duplicate or overlaid records in their system, estimated to be close to 15%. The hospital was able to eliminate annual large scale medical record clean-ups which cost the institution $1.8 million and involved over 250,000 duplicate records. Additional benefits included the elimination of the patient clipboard paperwork and reduction in medical errors.

- Memorial Hospital, North Conway, New Hampshire. Memorial Hospital reduced admission errors from 6% of patient records to less than 1% by deploying smart cards, including the reduction of medical record error from a rate of 7% to less than 1%, creating an annual savings of $55,000 for a 35 bed hospital. Patients saw a direct benefit as Memorial Hospital was able to reduce their admission time from 22 minutes to less than 3 minutes – an immediate cost savings of $574,000 in annual employee payroll minutes, which allowed Memorial to redirect staff to other productive tasks.

3. **What type of investment would be required to implement a smart card system in Medicare? If CMS were to move forward and implement a smart card system for the Medicare program, how can we ensure the integrity of the system from outside threats?**

The cost of the pilot program set up in the Medicare Common Access Card Act (H.R. 2925, 112th Cong.) is $29 million, which would fund a pilot program to be held in at least 5 geographic areas in which the Secretary of Health and Human Services (HHS) determines there is a high risk for waste, fraud, or abuse.

Recently, the Smart Card Alliance, an industry non-profit 501 (c)(3) education foundation and trade association, worked with an independent auditor to determine the full cost of deploying a nation-wide smart card based Medicare card system for both providers and beneficiaries *(see attached, DeLeon & Stang Medicare Report)*. The audit was completed in March 2012 with the intent to assist Congress and the CMS in their efforts to understand the true cost and actual savings of a nation-wide Medicare CAC deployment.

The audit found there are many different elements that must be considered as part of a national Medicare CAC deployment. Because the system will determine real-time eligibility of both providers and beneficiaries, it requires more than just the use of a smart card. Backend infrastructure and readers must be accounted for in any cost estimate. The estimate accounts for 2.6 million providers and 48 million beneficiaries for an overall total of 50.6 million participants.

Because providers will be going through an enrollment process and their biometric information will need to be captured the cost per provider within the system is estimated to be $31.08 per provider. For the beneficiary, the cost is somewhat less, $14.57 per beneficiary, because the beneficiary will receive their smart card via U.S. mail without the requirement of enrollment of biometric capture. The PIN code for the beneficiary could come pre-set as the last four digits of their Social Security number and could easily be changed, if the beneficiary desired upon first use.

The total cost for nationwide deployment of Medicare CAC system averages out to $24.24 per participant for a grand total of $1.3 billion for full deployment. These costs are completely inclusive for full deployment and should be evaluated against the return in reductions in fraud, waste and abuse. If Congress were to implement a smart card technology solution – such as described in the Medicare Common Access Card Act – it would have the potential to save American taxpayers over half of the estimated $60 billion per year cost of fraud. With over 48 million seniors, that comes out to approximately $1,250 of fraud per recipient per year. However, for a one-time investment of less than $25 per beneficiary, the federal government will realize a cost savings of over $612.50 per beneficiary per year – a return on investment 24 times over.

By their very nature, smart cards are extremely well-equipped to protect a nation-wide Medicare CAC system from outside threats. With that said, both privacy and security must be considered fundamental design goals for any personal ID system and must be factored into the specification of the ID system's policies, processes, architectures, and technologies. The use of smart cards strengthens the ability of the system to protect individual privacy and secure personal information.

Unlike other identification technologies, smart cards can provide authenticated and authorized information access, implementing a personal firewall for the individual and releasing only the information required when the card is presented. Smart card technology provides strong privacy-enabling features for ID system designers, including the ability to:

- Support anonymous and pseudonymous schemes
- Segregate multiple applications on the card
- Support multiple single-purpose IDs
- Provide authentication of other system components
- Provide on-card matching of cardholder verification information
- Implement strong security for both the ID card and personal data

Smart cards trust nothing until proven otherwise. For example, smart cards can require cardholders to authenticate themselves first (with a PIN or biometric) before the cards will release any data. And smart cards support encryption, providing patient data privacy and enabling at-home or self-service applications in suspect or untrusted environments to be secure.

The smart card's embedded secure microcontroller provides it with built-in tamper resistance and the unique ability to securely store large amounts of data, carry out own on-card functions (e.g., encryption and digital signatures), and interact intelligently with a smart card reader.

If the card is lost, the data on the card is secure and not readable without the individual's PIN code. Further, all information stored in the card cannot be read unless accessed via an authorized, authenticated reader. An attempt to hack the chip on the card would destroy the information in the process, because the chips are designed to shut down under brute force attacks. Once the card is reported lost or stolen the system will no longer recognize it and it becomes completely useless. One of the significant benefits that will reduce medical ID theft is that the card will no longer have the beneficiary's social security number printed on it.

No technology is unassailable nor is any system fool-proof. Smart cards as an identification technology, however, are the most mature, robust and secure systems on the market, and will continue to be well into the future, making it the optimal choice for a program such as Medicare.

4. **Recently, CNBC ran an expose on HEAT Teams assigned by the Inspector Generals' office to go after those committing fraud within the system. When interviewed for the documentary Tom O'Donnell, special agent in charge in the New York regional office of the U.S. Department of Health and Human Services Office of Inspector General (HHS-OIG), said there is no end in sight to fraud and their work load. Can smart card help with this?**

It is my unequivocal belief that smart cards can help to eliminate a great deal of Medicare fraud. The key to solving this is prevention – keeping criminals from submitting claims into the Medicare system to begin with. Requiring both parties – the beneficiary and the provider – to authenticate and authorize the transaction before an electronically signed and encrypted confirmation can be sent to CMS for payment is the key to the prevention of fraud. By implementing a Medicare CAC, critical resources will be freed up for HEAT Teams to fight other types of fraud that are just as damaging to the Medicare system.

5. **Please provide examples of how this type of smart ID card technology is being used in the United States. In those areas of our economy where it has been implemented, what were the results?**

Smart cards are being used extensively throughout the United States, providing a secure platform for many critical applications both within government and in the private sector to support access, identity, payment and other applications. These applications include:

Healthcare

Healthcare organizations worldwide are implementing smart health cards supporting a wide variety of features and applications. Smart health cards can improve the security and privacy of patient information, provide the secure carrier for portable medical records, reduce healthcare fraud, support new processes for portable medical records, provide secure access to emergency medical information, enable compliance with government initiatives and mandates, and provide the platform to implement other applications as needed by the healthcare organization. Here is case study of Mount Sinai Medical Center's use of smart cards for healthcare applications, followed by a short list of other successful implementations that are successfully using smart cards.

*Mount Sinai Medical Center: A Case Study in Personal Health Smart Cards*[1]

One of the country's oldest and largest voluntary teaching hospitals, New York's Mount Sinai Hospital is a 1,171-bed tertiary-care teaching hospital, with a medical staff of nearly 1,800, treating patients in Manhattan's Upper East Side and Harlem. It is internationally acclaimed for excellence in clinical care, education and scientific research in nearly every aspect of medicine. Officials at Mount Sinai, recognizing the need for more effective ways to verify patient identity and facilitate clinical data exchange, partnered with Siemens, a leading healthcare technology vendor, to create the Personal Health Card (PHC) initiative.

Recognizing that a truly effective solution to the problems of identity verification and information exchange had to work across multiple organizations, Mount Sinai partnered with nine other participating institutions in the greater New York City area to create a regional HealthSmart Network. Mount Sinai began issuing patient photo identification smart cards with embedded microprocessor chips that can store patient information and can be routinely updated by health care professionals throughout the network. Healthcare providers in the network are Mount Sinai Hospital of Queens, Cabrini Medical Center, Elmhurst Hospital, Atlantic Health, North General Hospital, Queens Hospital, St. John's Riverside Hospital, Jersey City Medical Center and Settlement Health, a clinic in the East Harlem/El Barrio area.

The cards can store vital patient information such as demographics, allergies, current medications and laboratory results, and uses a patient photograph to aid in the verification process. On the administrative side, the PHC provides a singular, snapshot view of the patient's medical and personal information, which can be shared across the network among physicians and admission staff. The PHC cards can be read and updated at any institution in the network.

The cards can store vital patient information such as demographics, allergies, current medications and laboratory results, and uses a patient photograph to aid in the verification process. On the administrative side, the PHC provides a singular, snapshot view of the patient's medical and personal information, which can be shared across the network among physicians and admission staff. The PHC cards can be read and updated at any institution in the network.

*Problems Solved by the Mount Sinai Personal Health Card*

*Identity and Registration*

Accurate registration and identity verification can be extremely challenging in a large urban hospital like Mount Sinai. With its large ethnic population, there are many common names. For example, if hospital officials searched their records for Juan Gonzalez, there might be 100 patients with that name in the database. Making sure they have the right Mr. Gonzales in front of them is the problem.

The PHC provides institutions in the network with positive visual identification of the patient, through comparison of the patient who is presenting the card with the photograph on the card.

[1] Adapted from the Mount Sinai Medical Center/Smart Card Alliance profile of its smart card implementation, 2007.

The card also provides a direct link to the patient's medical record number printed on the face of the card as both a number and a barcode. The card includes the patient's full name, which improves registration efficiency and accuracy.

*Immediate Access to Accurate Medical Information*

From EMTs to emergency room personnel to specialists and other physicians, everyone in the continuum of care needs immediate access to accurate information such as the patient's medical history, allergies to medications, and prescription and over-the-counter drugs taken. According to a recent study conducted by the Boston Consulting Group, as much as 40% of patient information is missing when it is needed by a medical professional for proper care. Also, a 2006 report published in the Journal of the American Medical Association found that adverse drug interaction along with medical errors result in an estimated 225,000 deaths per year.

The PHC solves the issue of medical information accuracy by providing accurate, up-to-date information that can be accessed immediately at the point of care, a huge benefit for both patients and healthcare providers.

*Cost Savings and Payment*

The registration process is also critical for proper billing and revenue capture. Two of the most common reasons for claims denials are incomplete demographic and insurance information, costing a healthcare institution millions of dollars in lost or delayed revenue. The process of reviewing and resubmitting old claims can also be an expensive process since it often requires detailed chart reviews and outreach to patients and physicians for additional information. The revenue cycle at Mount Sinai is highly dependent on the front-end registration process, which drives much of the downstream claims process. As much as 70% of the errors that contribute to pending and denied claims are attributable to issues with the registration process.

The PHC can greatly reduce medical record maintenance costs associated with errors from duplicate or commingled patient records. These errors occur when a new record is created for an existing patient, or the wrong patient record is selected. Reducing identity errors during patient registration can also greatly improve billing and collection processes and enhance revenue capture.

*Medicare/Medicaid and Fraud*

Mount Sinai has a large Medicaid/Medicare population that makes heavy use of its ambulatory clinics and emergency room. When registering for the first time, patients receiving clinic care must go through a financial screening process that documents their insurance coverage and verifies identity. Patients are then given a clinic card and are required to re-certify annually. Unfortunately, clinic cards and most Medicaid/Medicare cards do not have photographs. This has made it difficult for Mount Sinai employees to ensure that the patient named on the card is the actual patient in front of them. Patient fraud and abuse does exist, and it can be difficult to detect and harder to prevent with the clinic card process.

With the PHC, however, it becomes much more difficult to obtain healthcare services through fraudulent means, since the card includes a photo of the cardholder and requires use of a password and personal identification number known only by the cardholder.

*Information Sharing, Confidentiality and Privacy*

At Mount Sinai, all credentialed physicians have access to an array of clinical systems that house patient medical information, with systems able to be remotely accessed via a secured physician portal. However, other health care organizations in the network, as well as community-based clinics and private practice groups, do not have direct access to the clinical data. Data sharing among these groups can be uneven, commonly involving photocopied charts, faxed results and consultations and communication by telephone.

This critical problem is compounded by the fact that patients themselves can be unreliable sources of information, often forgetting or omitting important medical facts such as serious allergies, current medications, past procedures and chronic illnesses. Not having a good medical history can be serious and potentially life threatening. Mount Sinai also needs to maintain the privacy of health information as directed in the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

Mount Sinai officials believe that the PHC will significantly lessen many of these issues with identity and information sharing, increase privacy protection for patients, and help the organization to comply with HIPAA regulations. The ability to quickly and correctly identify patients and link them to complete medical records will benefit all stakeholders – patients, institutions, providers and payers. And the security features of the PHC will provide the highest levels of privacy protection.

Unlike normal ID cards that have no built-in security to protect the information printed on them, smart cards use the on-board computer chip and sophisticated cryptographic techniques to allow access to the information only to those authorized to see it. All patient data is stored on the chip in an encrypted format, and can only be accessed through the chip operating system with special software. Access privileges are set based on an individual's permission to see a specific type of information; for example, someone who is permitted to access identification and insurance information will not necessarily have access to medical information. Other built-in safeguards protect against tampering or creating counterfeit cards. Thus, the PHC helps network members comply with HIPAA regulations for keeping patient records and sharing patient data among physicians and emergency personnel. Privacy is also supported by limiting access to specific patient information, and by safeguarding its integrity and confidentiality.

*Language Issues and Electronic Health Records*

Language barriers can also hinder information gathering. Although Mount Sinai has staff who can provide translation services in many different languages, there is not always time for this in an emergency situation. There are also times when the patient is unconscious or unable to peak. As a result, healthcare providers can be forced to make critical decisions with little or no information.

The PHC helps to solve this issue because healthcare providers can access the medical information stored on the card, regardless of the patient's language or ability to speak. In addition, the PHC itself speaks the emerging standard "medical" language. Data storage protocols are compliant with the HL7 and the XML-based Continuity of Care Record (CCR) standards for electronic health records. HL7, a nonprofit organization, has developed widely recognized standards for the interoperability of electronic health care information, so it can be shared among various IT systems and applications. CCR is a related standard that allows physicians to easily create a sharable electronic health record containing the most relevant and timely core health information about a patient.

Mount Sinai's PHC implementation leverages smart card technology as a practical enabler that enhances the privacy and confidentiality of patient information and that provides easier access to patient information that is critical for both patient care and for healthcare administration. Only smart card technology puts the patient in control of their information and provides a robust solution that addresses the privacy and security concerns associated with personal healthcare information.

## *Queens Health Network – New York City*

The Queens Health Network (QHN) provides over 1 million ambulatory care visits annually to the 2 million residents of Queens, New York. QHN includes two leading acute-care facilities, Elmhurst and Queens Hospital Centers, 15 community-based medical centers and practices, and 6 school-based health centers. The network provides preventing and healthcare services throughout the borough.

Already paperless with electronic medical records (EMR) implemented at the two acute-care facilities, adopting smart cards was the next logical step in moving information in a more efficient manner – not just within their own healthcare system, but within their community. The card facilitates delivery of care by providing access to patient summary information in an emergency setting, which is especially helpful for patients whose primary language is not English.

In its first year, Elmhurst Health Connection cards were issued to approximately 14,000 patients within their Adult Primary Care service. Card issuance was seen as the first step in trying to share more patient information with physicians within their healthcare network, with smart cards a key element of their information infrastructure. Each card carries the patient's photo ID and conatain a 64 Kbyte chit containing data such as the patient's name, address, emergency contacts, allergies, current medications, and recent lab results. The cards are updated automatically at each patient visit.

The ability to read Smart Cards now extends beyond QHN's medical network facilities. Elmhurst Hospital Center received a $1.9 million HEAL New York Health Information Technology grant to pilot expansion of its Smart Card program by developing a reader that is now in every hospital emergency room in the borough of Queens. If a patient is rushed to a hospital outside the system, the attending physician will have the ability to access the patient's records using the Smart Card to ensure speedy and effective care that can save lives.

### *Lake Pointe Medical Center – Texas*

In 2008, Lake Pointe Medical Center successfully installed its smart card-based patient access system called throughout the facility. The smart card system had been developed for hospitals to quickly and accurately identify patients and help manage them through the admissions process. Patients with the smart card have the ability to view and contribute to their overall medical records, giving the provider a more complete medical picture. The smart cards used within the Lake Pointe Medical Center has been extended to some local physician offices who are affiliated with Lake Pointe, as well as local ambulance services who want to access the emergency information stored on the Smart card. Over 10,000 cards have been issued during the first year of the program at Lake Pointe.

### *The Memorial Hospital – New Hampshire*

New Hampshire's Memorial Hospital installed a similar smart card system in 2009. In its program, smart cards are issued and utilized during patient registration at The Memorial Hospital, as well as its three ancillary facilities. Each patient at Memorial is issued a branded The Memorial Hospital smart card; in the first year, total issuance exceeded 30,000 cards. The smart card stores patient demographic, insurance and medical information, allowing pre-registration and automated admission into the hospital. All information contained on the smart card is protected by sophisticated security encryption algorithms, making the data virtually impossible to steal.

Officials responsible for implementing the smart card system noted that, "We were provided with a universal patient identity smart card with connectivity between our disparate EMR's that authenticates our patient's identity and seamlessly integrated without changing our workflow. The results reduced admission time to less than a minute without paper, increased patient satisfaction to top 5% of all providers nationwide, diminished keystroke and billing errors, duplicate & overlay records and fraud over 95%. We were also able to reduce staff requirements over 25% with and ROI in less than 8 months."

U.S. Federal Government

Smart card technology is currently recognized as the most appropriate technology for identity applications that must meet critical security requirements. The U.S. Federal government has standardized on smart cards for employee and contractor identification cards and is also specifying smart cards in new identity programs for citizens, transportation workers and first responders.

*HSPD-12, FIPS 201 and the PIV Card*

Homeland Security Presidential Directive 12 (HSPD-12), issued by President George W. Bush on August 27, 2004, mandated the establishment of a standard for identification of Federal government employees and contractors. HSPD-12 requires the use of a common identification credential for both logical and physical access to federally controlled facilities and information systems. The Department of Commerce and National Institute of Standards and Technology (NIST) were tasked with producing a standard for secure and reliable forms of identification. In response, NIST published Federal Information Processing Standard Publication 201 (FIPS 201), Personal Identity Verification (PIV) of Federal Employees and Contractors, issued on February 25, 2005, and a number of special publications that provide more detail on the implementation of the standard.

Both Federal agencies and enterprises are now implementing FIPS 201-compliant ID programs and issuing PIV cards. The FIPS 201 PIV card is a smart card with both contact and contactless interfaces that is now being issued to all Federal employees and contractors. Within the next five years, GSA estimates that 12 million PIV cards will be used in the Federal Government alone, driving a significant expansion of FIPS 201 infrastructure and applications.

*Department of Defense Common Access Card*

One of the most advanced smart ID card programs in the United States is the Department of Defense Common Access Card, a smart card that serves as the DoD's standard identification for active duty military personnel, selected reserve personnel, civilian employees, and eligible contractor personnel. The CAC is the principal card used for logical access to DoD computer networks and systems, and will be the principal card used to enable physical access as systems are installed for authentication and access at DoD facilities. As with all Federal agencies, DoD is now migrating to a FIPS 201-compliant Common Access Card. While it is hard to measure fraud reduction within government agencies, the DoD confirms a 46% reduction in cybersecurity attacks on the first day of secured computer access implementation using smart cards.

*DHS First Responder Authentication Credential (FRAC)*

The Office of National Capital Region Coordination coordinated a major initiative to develop a smart identity card system (the First Responder Authentication Credential) for emergency responders. These smart cards would allow first responders from across the region the ability to quickly and easily access government buildings and reservations in the event of a terrorist attack or other disaster. The initiative is designed to remedy access problems such as those encountered by state and local emergency officials responding to the 9/11 attack on the Pentagon. So far, nine states have taken the lead to deploy FRAC credentials for first responders, with many more on the way. It should be noted that all doctors and nurses are considered first responders; as such a Medicare CAC provider card could serve double duty as a FRAC credential, even further reducing implementation costs.

*U.S. ePassport*

The Department of State, Bureau of Consular Affairs, in cooperation with its partners at the United States Government Printing Office and the Department of Homeland Security, is issuing the ePassport – a new version of the United States passport that contains an embedded contactless smart card chip. The chip is used to store biographic data on the passport; once unlocked, the data can be displayed on a screen at passport control. The new technology enhances the security of the passport and facilitates the movement of travelers at ports of entry. Since the first year of deployment, 2005, the State Department issued over 75 million ePassports containing the secure smart card chip.

*The American Medical Association/Centers for Disease Control Health Security Card*

The American Medical Association's Center for Public Health Preparedness and Disaster Response is working with Center for Disease Control and FEMA to develop a pilot program to show the benefit of a Health Security Card based on smart card technology for patients in the event a disaster or health emergency. Preliminary findings from the pilot excises show 90% of patient using the smart cards rated the care they received as good to excellent, with 75% affirming care as very good or excellent. In early 2013, the AMA will issue a final report on the smart card pilot.

## Financial Services

### *EMV Credit and Debit Payment*

Financial institutions in Europe, Latin America, Asia/Pacific, Canada and the United States are issuing contact smart cards using the dual-interface Europay-MasterCard-Visa (EMV) standard for credit and debit payment (commonly referred to as "chip and PIN") or will soon be migrating to EMV issuance. EMV smart cards will be introduced into the US market mid-2013. According to EMVCo,[2] over 1.5 billion EMV cards have been issued globally and over 21.6 million Point-of-Sale (POS) terminals accept EMV cards as of Q2 2012. This represents 44.1% of the total payment cards in circulation and 72.0% of the POS terminals installed globally, excluding the United States.

## Enterprise ID

### *Smart Cards and Logical Access*

Organizations of all sizes and in all industries are working to improve the process used to identify users to their networked systems. With the growing use of wired and wireless networks to access information resources and the increasing occurrence of identity theft and attacks on corporate networks, password-based user authentication is increasingly acknowledged to be a significant security risk. Both enterprises and government agencies are moving to replace simple passwords with stronger, multi-factor authentication systems that strengthen information security, respond to market and regulatory conditions, and lower support costs.

Smart cards support all of the authentication technologies, storing password files, public key infrastructure certificates, one-time password seed files, and biometric image templates, as well as generating asymmetric key pairs. A smart card used in combination with one or more authentication technologies provides stronger multi-factor authentication and significantly

[2] EMVCo manages, maintains and enhances the EMV Integrated Circuit Card Specifications to ensure interoperability and acceptance of payment system integrated circuit cards on a worldwide basis. EMVCo is owned and managed by American Express, JCB, MasterCard, and Visa. EMV specifications were first issued in 1996, with active working groups providing updates and revisions.

strengthens logical access security. Smart card technology also provides the flexibility for including all authentication factors in a single smart card, improving the security and privacy of the overall authentication process.

### *Smart Cards and Physical Access*

Smart cards are increasingly accepted as the credential of choice for securely controlling physical access. Standards-based smart ID cards can be used to easily authenticate a person's identity, determine the appropriate level of access, and physically admit the cardholder to a facility. Through the appropriate use of contact or contactless smart card technology in the overall physical access system design, security professionals can implement the strongest possible security policies for any situation.

More than one access application can be carried on a single smart ID card, enabling users to access physical and logical resources without carrying multiple credentials. Security can change access rights dynamically, depending on perceived threat level, time of day, or other appropriate parameters. Smart card support for multiple applications allows organizations to expand card use to provide a compelling business case for the enterprise. Smart cards not only secure access to physical or logical resources, they can store data about the cardholder, pay a fee or fare if required, certify transactions, and track ID holder activities for audit purposes. Because supporting system components can be networked, shared databases and inter-computer communication can allow separate functional areas in an organization to exchange and coordinate information automatically and instantly distribute accurate information over large geographic areas.

### *Enterprise ID Implementations*

The Smart Card Alliance created the following profiles and resources to showcase how organizations can successfully use smart cards for physical and logical access.

- Boeing
- Microsoft
- Rabobank
- Shell Group
- Sun Microsystems Java Badge

In January 2008, DataMonitor did research on the state of passwords and smart cards in the enterprise, and published the results in a white paper that shows the ROI for enterprise smart cards. The research found that 62% of enterprises experienced problems with passwords and that 40 man-hours per week would be saved using smart cards and single sign-on. The analysis concluded that a 2000-user company deploying smart cards could see a US$3.4 million savings over the course of 3 years.

## Identity Management

### *Smart Cards and Identity Applications*

Smart card technology is currently recognized as the most appropriate technology for identity applications that must meet critical security requirements, including:

- Authenticating the bearer of an identity credential when used in conjunction with personal identification numbers (PINs) or biometric technologies;
- Protecting privacy;
- Increasing the security of an identity credential;
- Implementing identity management controls.

Countries around the world use smart cards for secure identity applications. In addition, both government organizations and public corporations (including Microsoft, Sun Microsystems, Chevron, and Boeing) use smart employee ID cards to secure access to physical facilities and computer systems and networks.

*Identity in Cyberspace*

U.S. citizens are increasingly using the Internet for sensitive transactions, like banking, mortgage applications, buying and trading stocks, and reviewing healthcare information. Given this, there are very real problems of identity management, privacy and security in cyberspace. Smart card technology (in various form factors including cards, USB tokens and mobile phones) enables strong multi-factor authentication on the Internet.

The Obama administration has recognized the need for stronger online identity authentication and established the National Strategy for Trusted Identities in Cyberspace (NSTIC) initiative. NSTIC broadly defines an Identity Ecosystem that would re-establish trust and better protect online identities. According to the Howard A. Schmidt on the White House blog, "Through the strategy we seek to enable a future where individuals can voluntarily choose to obtain a secure, interoperable, and privacy-enhancing credential (e.g., a smart identity card, a digital certificate on their cell phone, etc.) from a variety of service providers–both public and private–to authenticate themselves online for different types of transactions (e.g., online banking, accessing electronic health records, sending email, etc.)."

## Telecommunications

Smart cards are used extensively in the telecommunications industry worldwide. The Smart Card Alliance has reported that 5.2 billion smart cards will ship globally for telecommunications applications in 2012. The Smart Card Alliance is estimating that smart card shipments for telecommunications applications will grow to 5.45 billion in 2013.

Smart cards are used in two primary telecommunications applications – as prepaid (stored value memory cards) telephone cards and as the microprocessor smart card-based Subscriber Identity Module (SIM) in mobile phones. In addition, new NFC-enabled mobile phones that incorporate a secure element are being used for a variety of applications, including mobile contactless payments, ticketing and mobile marketing.

*Smart Cards, SIMs and UICCs*

A Subscriber Identity Module (SIM) card is a type of microcontroller-based smart card used in mobile phones and other devices. A SIM identifies and authenticates a subscriber to a wireless cell phone network. Unless blocked by the operator, a subscriber can move his phone service to a new phone just by physically moving the SIM. SIMs also facilitate global roaming, providing subscribers with access to voice, data and other services when traveling in other countries. In addition, SIMs can store contact information and phone numbers, and can be used for other applications.

The Universal Integrated Circuit Card (UICC) is a new generation of SIM technology optimized for newer wireless network standards. The term SIM is widely used in the industry and especially with consumers to mean both SIMs and UICCs, although they are different technologies. The UICC offers many enhanced capabilities, including better support for multiple applications and IP addressing.

SIMs and the newer UICCs are used in wireless networks based on several different standards, but the fact that they are mandatory in GSM (Global System for Mobile communications) networks has been a very significant market driver.

SIMs and UICCs are the smart card industry's highest volume products for both units and revenue. According to Eurosmart, microcontroller smart card production shipments for the telecom sector in 2012 will be 5.2 billion units. This represents 73% of the 7.095 billion total smart cards that are estimated for all sectors for 2012.

*Pay Phones and Smart Cards*

Over 100 countries use smart cards instead of coins in their pay phones to improve customer convenience and telecommunications operators' business models (less cash, reduced risk of losses).

*NFC-Enabled Mobile Applications*

NFC technology is a standards-based wireless communication technology that allows data to be exchanged between devices that are a few centimeters apart. NFC operates at 13.56 MHz and transfers data at up to 424 Kbits/second.

NFC is distinguished by its intuitive interface and its ability to enable largely proprietary wireless networking platforms to interoperate in a seamless manner. The primary uses are to:

- Connect electronic devices, such as wireless components in a home office system or a headset with a mobile phone;
- Access digital content, using a wireless device such as a cell phone to read a "smart" poster embedded with an RF tag;
- Make contactless transactions, including those for payment, access and ticketing.

Expected NFC-enabled mobile applications include:

- Making payments with a wave or a touch anywhere contactless card readers have been deployed;
- Reading information and "picking up" special offers, coupons and discounts from smart posters or smart billboards;
- Storing tickets to access transportation gates, parking garages or get into events;
- Storing personal information that will allow secure building access.

When used for mobile contactless payment, NFC-enabled mobile phones incorporate smart chips (called secure elements) that allow the phones to securely store the payment application and consumer account information and to use the information as a "virtual payment card." NFC payment transactions between a mobile phone and a POS terminal use the standard ISO/IEC 14443 communication protocol currently used by EMV and U.S. contactless credit and debit cards.

NFC-enabled mobile phones can also be used for chip-enabled mobile marketing applications – coupons, loyalty programs and other marketing offers that can add significant value for merchants, issuers and the mobile ecosystem.

## Transportation

Smart cards are used worldwide in transportation applications, with millions of smart cards in use for both transit fare payment and parking fee payment.

*Smart Cards and Transit*

Mass transit agencies worldwide have been using stored value prepaid cards for electronic ticketing since the 1970s. Through the late 1990s, this market steadily began transitioning from magnetic stripe technology to contactless smart cards. Today, virtually all transit fare payment systems use contactless smart cards as the primary ticket medium. Major deployments are already operational in cities around the world, including Hong Kong, Seoul, Pusan, Washington, D.C., and Shanghai.

Since the late 1990s, U.S. transit agencies have made significant investments in contactless smart card-based automatic fare collection (AFC) systems, with over $1 billion in contracts awarded for new systems that incorporate the latest developments in information technology (IT). Most of these systems use agency-branded contactless smart cards as the primary fare medium. Most major U.S. metropolitan areas now have closed-loop, stored value contactless smart card-based AFC systems including: Washington, D.C.; San Francisco; Oakland; Los Angeles; Chicago; San Diego; Seattle; Minneapolis; Houston; Boston; Philadelphia; Atlanta; and the New York/New Jersey area.

In addition to these transit-specific fare payment systems, transit agencies in the U.S. are moving to open bank card payments for fare payment at the the point of entry to subways, trains and buses. Beginning in January 2009, the Utah Transit Authority implemented the first complete open bank card payment system for transit fare payment in the United States. Transit operators in the New York–New Jersey region (MTA New York City Transit, Port Authority Trans Hudson (PATH) and New Jersey Transit) collaborated on a pilot to test the concept of open payments on two subway lines, several connecting bus routes in New York, and bus routes and connecting service to the PATH system in New Jersey. Currently, transit agencies in numerous locations, including Philadelphia, Chicago, Washington, DC, Dallas, and Toronto are actively pursuing open payment solutions.

*North American Transit Smart Card Projects and Implementations*

The following are active transit smart card implementations in the U.S. and Canada:

- Atlanta / MARTA Breeze Card
- Baltimore / MTA CharmCard
- Boston / MBTA Charlie Card
- Chicago / CTA (Chicago Card and Chicago Card Plus)
- Houston / METRO Q Card
- Los Angeles / LACMTA TAP Card
- Miami / MDT EASY Card
- Minneapolis-St. Paul / Metro Transit Go-To Card
- Montreal, Quebec / STM OPUS Card
- New Jersey / NJ TRANSIT Tap>Ride
- Newark / PANYNJ (SmartLink)
- Port Authority Trans Hudson (PATH)
- Philadelphia / PATCO FREEDOM Card
- Salt Lake City / UTA EFC Card
- San Diego / MTDB Compass Card
- San Francisco / MTC (Clipper Card)
- Seattle-Puget Sound / KC Metro ORCA Card
- Toronto, Ontario / Metrolinx PRESTO Card
- Ventura County

- Washington, DC / Washington Metropolitan Transportation Authority SmarTrip

In addition, several transit agencies are in active procurements for open payment systems that accept contactless bank cards. These include:

- Chicago / CTA
- Dallas / DART
- New York City / MTA New York City Transit
- Philadelphia / SEPTA
- Washington, DC / WMATA

*International Transit Smart Card Projects and Implementations*

Selected active international transit smart card implementations are listed below.

- Hong Kong Octopus Card
- London Oyster Card

*Smart Cards and Parking*

The use of contact smart card technology is well established in the parking market, with parking equipment vendors providing solutions for all segments: single-space meters, multi-space meters, and off-street parking.

In addition to contact smart card-based programs, transit agencies using contactless smart cards for fare payment are expanding the use of the card to pay for parking. Active programs in the U.S. include: WMATA SmarTrip; Port Authority Transit Corporation (PATCO), operating in Pennsylvania and New Jersey; and the Metropolitan Atlanta Rapid Transit Authority (MARTA).

6. **What other countries are using smart cards for healthcare? And why have these countries chosen smart card technology after evaluating all the possibilities?**

A number of nations have implemented smart card-based healthcare systems for many reasons beyond fraud reduction, such as security and ensuring administrative cost savings.

French healthcare system SESAM-Vitale.

The French government implemented smart cards in order to verify who was receiving treatment and to quickly provide reimbursements within three to five days as opposed to 3-4 weeks. As a result, the processing cost of a claim within the system was reduced from 1.74 Euros to .27 Euros. With over one billion transactions per year, the transition saves the system over 1.4 billion Euros/year.

German Ministry of Health.

Germany deployed secure smart healthcare cards to approximately 70 million beneficiaries and is currently deploying about 280 thousand health professional cards. The projected achievable program savings in the German national program range from 1.7 to 2.9 billion Euros per year, of which between 800 million to two billion Euros would come from fraud reduction. According to the German Ministry of Health in January 2012, the beneficiary deployment alone has generated annual fraud reduction of 250 million Euros. Provider fraud reduction data will not be available until deployment is completed next year.

Taiwan.

The Taiwanese government implemented one of the longest standing and most comprehensive secure health care cards in the world. Implemented in 2004, the program has issued 24 million patient cards and 300 thousand provider cards. The card data includes not only insurance information but medical information as well. The Bureau of National Health in Taiwan reports that moving from paper to a secure smart card has extended the life of cards by 5-7 years, reduced fraud, saved on administrative costs, and reduced health care spending in general. Taiwan's administrative costs are the lowest in the world at two percent (compared to the U.S. at 31 percent).

**7. Explain how open technology standards work and what non-proprietary means in the context of government established standards for smart cards?**

Open technology standards are critical for the wide-spread adoption and use of any technology, but especially so for smart cards. These standards are developed by international organizations, of which the U.S. government is often a party, to ensure multiple use cases and robust security. Because smart cards are developed via internationally accepted open-standards, they can be built and implemented by anyone following the standards without limitation.

Implementations using open-standards are especially valued because the underlying technology is non-proprietary, and is thus not vulnerable to monopoly abuses by vendors using non-standard technologies. For instance, implementing a proprietary system means that client (in this case CMS) would be forced to use only the vendor who owns the proprietary technology, and be locked into choosing from their limited technology solutions, as well as their pricing schemes. Should the relationship with the proprietary vendor not work out, the client is then forced to redesign the system – from computers to readers to the very cards themselves – if they wish to end the relationship. Also, there is the prospect that the vendor may be bought by a company that the client may not wish to do business with (a foreign company, for example) or may go out of business outright. Neither of these situations are beneficial to the client, nor its customers (beneficiaries and providers in this case) or those actually funding the project – the American taxpayer.

By using a standards-based approach, the U.S. government can be assured that it is not subject to the above mentioned problems. Also it can put such a smart card project out to bid with the knowledge that since anyone can build to the standard, its costs will be significantly lower and the quality of the end product will be higher due to increased competition. A vendor using open-standards will work especially hard to produce favorable results, for if they do not, the project can be easily re-bid to other vendors desiring the business. Further, standards organizations are constantly working to improve and strengthen the standards against security threats. Proprietary systems may also work to improve their product, but the incentive is lower, as the client is locked-in to the sunk costs of the proprietary system and will be unwilling to lose their investment by switching vendors. Fortunately, the U.S. government has a long history of not only encouraging the use of open-standards, but mandating it. The smart card implementations used by the federal government are an excellent example of this.

Smart card systems that would be used for a Medicare CAC would be built to exacting standards. Below are standards, directives and laws that guide smart card implementations, as well as information on the organizations responsible for them:

> *Federal Information Processing Standard 201 – FIPS 201*
> As a result of Homeland Security Presidential Directive 12 (HSPD-12), issued by President George W. Bush on August 27, 2004, NIST published Federal Information Processing Standard Publication 201 (FIPS 201), Personal Identity Verification (PIV) of Federal Employees and Contractors, on February 25, 2005. FIPS 201 provides the specifications for a standard Federal smart ID card, called the PIV card, that must be used for both physical and logical access and can be used for other applications as determined by individual agencies. The PIV card is a smart card

with both contact and contactless interfaces. Government agencies are currently implementing FIPS 201-compliant systems.

*Other Federal Information Processing Standards (FIPS)*
FIPS standards are developed by the Computer Security Division within NIST. FIPS standards are designed to protect Federal computer and telecommunications systems. The following FIPS standards apply to smart card technology and pertain to digital signature standards, advanced encryption standards, and security requirements for cryptographic modules.

*The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (Public Law 104-191)*
This law states that the Secretary of Health and Human Services (HHS) is to adopt national standards for implementing a secure electronic health transaction system. Examples of these transactions include: claims, enrollment, eligibility, payment, and coordination of benefits. The goal of HIPAA is to create a secure, cost-effective means for individuals to efficiently accomplish electronic health care transactions. HHS has designated the Centers for Medicare and Medicaid Services the responsible entity for enforcing HIPAA.

*Digital Signatures*
FIPS 186-2 specifies a set of algorithms used to generate and verify digital signatures. This specification relates to three algorithms specifically, the Digital Signature Algorithm (DSA), the RSA digital signature algorithm, and the Elliptic Curve Digital Signature Algorithm (ECDSA) algorithm.

*Advanced Encryption Standards*
FIPS 197: The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt and decrypt information.

*Security Requirements for Cryptographic Modules*
FIPS 140: The security requirements contained in FIPS 140 (currently version 2) pertain to areas related to the secure design and implementation of a cryptographic module, specifically: cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

*International Standards Organization (ISO)/International Electrotechnical Commission (IEC) Standards*
ISO/IEC is one of the worldwide standard-setting bodies for technology, including plastic cards. The primary standards for smart cards are ISO/IEC 7816, ISO/IEC 14443, ISO/IEC 15693 and ISO/IEC 7501.

*American National Standards Institute (ANSI) Standards*
ANSI recommends standards directed to the needs of the U.S. and supervises standards-making activities. It does not write or develop standards itself. Thus, in the U.S., any group that participates in ISO must first participate in ANSI. The International Committee for Information Technology Standards (INCITS) serves as ANSI's Technical Advisory Group (TAG). Working groups within INCITS – such as B10 (Identification Cards and related devices), T6 (Radio Frequency Identification Technology) and M1 (biometrics) contribute directly to ISO groups (for example, the ISO/IEC Joint Technical Committee 1/Subcommittee 17 (JTC 1/SC 17)).

*GlobalPlatform*
GlobalPlatform (GP) is an international, non-profit association. Its mission is to establish, maintain and drive adoption of standards to enable an open and interoperable infrastructure for smart cards, devices and systems that simplifies and accelerates development, deployment and

management of applications across industries. According to GlobalPlatform, as of 2009, an estimated 305.7 million GlobalPlatform-based smart cards had been deployed across the world, with an additional 2 billion GSM cards using GlobalPlatform technology for over-the-air (OTA) application download.

*Common Criteria*
Common Criteria (CC) is an internationally approved security evaluation framework providing a clear and reliable evaluation of the security capabilities of IT products, including secure ICs, smart card operating systems, and application software. CC provides an independent assessment of a product's ability to meet security standards, with the goal of giving customers confidence in the security of IT products and leading to better decisions about security. Security-conscious customers, such as national governments, are increasingly requiring CC certification in making purchasing decisions. Since the requirements for certification are clearly established, vendors can target very specific security needs while providing broad product offerings. CC has been adopted and is recognized by 14 countries.

*G-8 Health Standards*
The G-8 countries have come together to develop a standard format for populating data on a health card. This standard attempts to create interoperability across health cards from the G-8 countries. It addresses file formats, data placement on the card, and use of digital certificates in health care.

*EMV 2000*
EMV is an open-standard set of specifications for smart card payments and acceptance devices. EMVCo, owned by American Express, JCB, MasterCard, and Visa, manages, maintains and enhances the EMV specifications, to ensure global interoperability of chip-based payment cards with acceptance devices including point of sale terminals and ATMs.

*Personal Computer/Smart Card (PC/SC) Workgroup*
The PC/SC Workgroup was formed in 1996 and included Schlumberger Electronic Transactions, Bull CP8, Hewlett-Packard, Microsoft, and other leading vendors. This group has developed open specifications for integrating smart cards with personal computers. The specifications are platform-independent and based on existing industry standards. They are designed to enable application developers to create smart card-based secure network applications for banking, health care, corporate security, and electronic commerce. The specifications include cryptographic functionality and secure storage, programming interfaces for smart card readers and PCs, and a high-level application interface for application development. The specifications are based on the ISO/IEC 7816 standard and support EMV and GSM application standards.

*Healthcare Cards*
The Workgroup for Electronic Data Interchange (WEDI) was established to provide leadership and guidance to the healthcare and healthcare insurance industries on how to use and leverage its collective knowledge, expertise and information resources to improve the quality, affordability and availability of electronic healthcare standards as required by the Health Insurance Portability and Accountability Act (HIPPA). In June 2011, WEDI unveiled its Health Card Implementation Guide, which identifies smart cards as the standard for health identification cards.

*Biometric Standards*
Many new secure ID system implementations are using both biometrics and smart cards to improve the security and privacy of the ID system. There are over 12 standards in use for biometrics developed by ANSI.

8. **Can you please provide to the committee a list of the fraud prevention areas that you believe could be improved within CMS? If these areas include deficiencies on the part of CMS, can you**

**provide explanation as to why you believe those deficiencies exist? Can you also provide recommendations on ways that CMS fraud prevention can be improved?**

There are many ways that fraud, waste and abuse are being attacked within CMS, including voluntary citizen reporting systems, tougher sentences for criminals, enhanced screening and other enrollment requirements, increased coordination of fraud prevention efforts between government agencies, and the Health Care Fraud Prevention and Enforcement Action Team (HEAT). Additionally, there has been a new focus on compliance and prevention of Durable Medical Equipment providers, the increased use of medical Recover Audit Companies to recover Medicare overpayments, and back-end analytic systems that attempt to detect fraud. Unfortunately, fraud continues to plague the Medicare system, with losses anywhere from *$60 - $110 billion per year.*

The actual cost to American taxpayers is not known due to the lack of effective fraud reporting and accounting, but is expected to be much higher for a number of reasons. For instance, the costs of pursuing, catching, and prosecuting fraudsters by the federal government must also be included in the rising cost of Medicare fraud. Specifically, to advance the use of predictive analytics technologies to help prevent fraud in the Medicare program, the Small Business Jobs Act of 2010 appropriated $100 million to CMS for its development and implementation. In addition, the GAO testified to this Subcommittee in November that in fiscal year 2011, the federal government allocated at least $608 million in funding to investigate and prosecute alleged cases of Medicare fraud. These figures must also be added in when evaluating the real cost of fraud to the Medicare system and the American taxpayer.

Despite what is being done so far, it is not enough. HHS recently reported that $4.1 billion in fraud losses were recovered in 2011 thanks to successful prosecutions. This number, however, pales in comparison to the $60-110 billion lost to fraud every year. If anything, these figures argue that back-end solutions need to be augmented by strong, preventative actions.

A smart card-based Medicare CAC would significantly support these efforts by *preventing fraud and increasing accountability on the front-end.* By requiring beneficiaries and providers to authenticate themselves as authorized to participate in the program, and mutually authenticate the transaction *before* it is ever presented to CMS for payment, we conservatively anticipate that fraud losses will be cut in half. The impact will be felt immediately; not only would additional resources will be freed up for enforcement purposes, but the integrity of the Medicare system would be ensured for years to come. With discussions of reducing benefits or raising taxes to ensure Medicare's survival, all efforts to prevent the outflow of precious Medicare funds to criminals should be taken.

**The Honorable Marsha Blackburn**

1. **CMS has implemented a number of measures to reduce fraud and improper payments both as part of the Patient Protection and Affordable Care Act and Small Business Jobs Act of 2010. How would Medicare CAC complement Medicare's current prepayment control efforts and what benefits would such a system provide to the current practice?**

Medicare CAC can be best thought of as acting as a gatekeeper to CMS. Building off the answer to Congressman Pitt's question #8 *(above),* a smart card-based Medicare CAC would prevent unscrupulous fraudsters from presenting fake claims to Medicare in the first place. The systems currently in place, while useful in fighting fraud after a claim has already been presented (and in most cases, paid), are overwhelmed by the volume of claims being put through to CMS. The Medicare CAC program, however, would prevent false claims from being put through as only legitimate providers would possess a valid CAC card in which to initiate the claims process. Even if a certified provider were to have their certification revoked by CMS, the Medicare CAC would still ensure the integrity of the program as the now de-certified providers' card would be remotely de-authorized and unable to conduct a transaction.

A report released on January 24, 2013 by the HHS Office of the Inspector General (OIG) on improper Medicare payments shed light on an incident where the Medicare CAC would have helpful in saving taxpayer money. The HHS OIG report found that CMS made $33,587,634 in improper payments on behalf of 11,619 incarcerated beneficiaries between 2009 and 2011. Medicare typically does not pay for services for incarcerated beneficiaries (42 CRF S 411.4(b)); however, federal requirements allow Medicare payments for incarcerated beneficiaries if state or local law requires the incarcerated person to repay the state medical costs. The Medicare beneficiaries that fall into this category are marked with exception codes; the improper payments, however, were made on behalf of those without codes. Using Medicare CAC, CMS would've been able to update the incarcerated beneficiary's account information in a timelier manner, helping to avoid inadvertent billing mistakes as well as preventing outright fraud.

The trustees of the Medicare program forecasted in April 2012 increased financial troubles as a result of an aging population and rising health care costs, predicting that Medicare's hospital fund would begin to run out of money beginning in 2024. Additionally, they reported that the hospital fund will pay out $38 billion more in benefits than it collects in taxes and premiums from seniors and the disabled. Medicare CAC has the potential to prevent that amount in losses, further strengthening the chances for Medicare's long-term survival.

**2. In the hearing a number of claims were made regarding the vulnerabilities of smart cards. Can you respond to these concerns and how a Medicare smart card pilot would mitigate against these alleged vulnerabilities.**

Many of the claims made at the hearing regarding the vulnerabilities of smart cards were anecdotal at best, and unsupported by an appropriate factual, scientific analysis. While no system can ever be considered invulnerable, smart cards are a tried, tested and trusted technology proven to be extremely resistant to attack.

Dr. Fu's comments at the hearing focused mainly on newspaper reports of suspected attacks. Dr. Fu's 2007 published work in this area focused on finding exploits and vulnerabilities in the infrastructure around ISO 14443 RFID contactless cards, which are not widely used today. The ISO 14443 standard for RFID is used specifically for inventory purposes in warehouse environments, and is inappropriate and not recommended for identity management purposes. Medicare CAC, on the other hand, would use a contact smart card, utilizing the ISO 7816 standard, so I don't believe his research is on point nor is it up-to-date with the current state of the technology.

It is important to note, however, that Dr. Fu's testimony is at odds with recommendations he made in a recent journal article. In it, he specifically endorses smart cards as an authentication token for use in implantable medical devices to protect them – and the patients using them – against attack when tied to medical professional's identity. He further asserts that requiring such tokens could further limit unauthorized parties' use of medical equipment.[3] Regardless, Dr. Fu raised a number of issues in his testimony that we welcome the opportunity to address.

*Chinese Attack on Department of Defense Computer*

Most recently, it was reported that a Chinese computer virus hacked into DoD computers connected to smart card readers to steal PINs from DoD smart cards. The attack installed keyloggers by tricking personnel into viewing an emailed PDF file containing an exploit ("New Sykipot variant can steal PINs from DoD smart cards," GCN, January 13, 2012).

In reality, the cardholder's PIN is useless without physical possession of the associated card, inserted into a secure terminal. Further, the hackers behind the virus could only access systems

[3] ,Daniel Halperin, Thomas S. Heydt-Benjamin, Kevin Fu, Tadayoshi Kohno, and William H. Maisel, Security and Privacy for Implantable Medical Devices, Pervasive Computing, IEEE Computer Society, Vol. 7, No. 1 January–March 2008, at 36.

only as long as an infected user's card remains logged into a system. Once the card was removed, as is required when leaving a DoD computer unattended for any length of time, the vulnerability is over. It should be noted that the attack was not on the card itself, but sent via email to a user who unsuspectingly opened an unfamiliar email to infect the system.

A Medicare CAC system, on the other hand, would be a somewhat closed system comprised of the beneficiary's card, the provider's card and the authorized card reader itself. Only when those three components are together will a confirmation message be generated, which would be a digitally signed and encrypted notification to CMS saying the transaction has been approved by all parties and is appropriate to pay. Further, the notification would be accompanied by a unique hash value that would be verified by the CMS servers as being authentic to that particular transaction, and that transaction only. It cannot be used for other transactions, further strengthening the integrity of the system.

It should also be noted that the DoD systems present an exceptionally high-value target for intrusion – especially for this attack – which could not have been attempted without the assistance or direction of a well-funded foreign intelligence agency. Comparatively, an attempt to attack a single Medicare billing transaction to defraud CMS would be extremely impractical and unlikely, even with the assistance of foreign intelligence agencies.

*California Legislator's ID Hack*

In 2006, a California legislator had her contactless State ID card sniffed and cloned by white hat hacker (hired by California Assemblyman Joe Simitian) to illicitly enter the California Statehouse. While making for an interesting story, the attack focused on an unsecured, unencrypted RFID card, not a secure, encrypted smart card that is activated only through a PIN and certified reader. As RFID technology was developed to help track inventory in warehouses, it was developed to be easily found and read; as such it is an inappropriate technology to use for an identification card, and would not ever be in contention for use within Medicare CAC.

*Contactless Credit Card Hack*

Again in 2006, Dr. Fu tested 20 contactless credit cards from Visa, MasterCard and American Express. He reports being able to skim and store the cardholders' name and other data, as the data was unencrypted and stored as plain text. In a laboratory setting with sophisticated equipment run by doctoral students, it is possible to skim information from a contactless smart card only if the information on the card was stored "in the clear." This exploit revealed a vulnerability not in the technology but in the implementation, as it was the credit card company's fault for not following basic security rules in protecting consumer data. Thankfully, standards, technologies and practices have increased exponentially in the seven years since Dr. Fu's laboratory experiment.

*Chip and PIN smart card hacks*

Another claim raised was that EMV payment cards are susceptible to "pre-play attack" at point-of-sale (POS) terminals. Only ATM/POS implementers who fail to use random number for authentication and opt for using a counter, timestamp or home-grown algorithm are susceptible. Again this is an implementation problem; accepted practice is to use what's known as a 'nonce', which in security engineering is an arbitrary number used only once in a cryptographic communication, and never use that number again.

**3. Other technology solutions (e.g., magnetic-stripe, bar code, smart phones, mobile applications) have been suggested as potential solutions to reduce fraud within Medicare at possibly a lower cost. Please compare the benefits of smart card solutions for Medicare as compared to other proposed solutions.**

A Medicare CAC smart card system has the benefit of being the product of over thirty years of design and implementation success, which includes advanced cryptographic engineering. While many of the solutions mentioned in your question (e.g., magnetic-stripe, bar code, smart phones, mobile applications) have been around quite a while, they all however have significant inherent vulnerabilities.

Magnetic stripe cards, while they too have been around since the 1960's, are notoriously susceptible to cloning. Because there is no security or encryption on mag-stripe cards, criminals can run a stolen mag-stripe card through an inexpensive reader, capture the information, and produce *thousands* of counterfeit cards in a single sitting. Bar codes present a similar problem, as they can be photocopied or scanned and printed on to multiple cards. Use of either of these systems would defeat the anti-fraud purposes of implanting a Medicare CAC system. In fact, banks and financial services companies across the globe have abandoned mag-stripe cards for this very reason, adopting instead smart card solutions. Similarly, the U.S. financial services sector will be migrating to a smart card solution for credit and debit cards starting this year.

Smart phones and mobile applications have the potential to be used, but unfortunately at this time, they are an unproven technology for these types of transactions. While smart phones do possess a smart card SIM chip in them, the chip is dedicated to authenticating the phone to the telecommunications network and cannot be used for other purposes. Efforts are currently under way to enable smart phones to be able to transact financial transactions using another smart card chip, known as the secure element. This type of near field communications (NFC) payment mechanism is in some smart phones, but as of yet they are not sufficiently in the marketplace to make them a viable implementation option.

While a promising prospect for future use, another barrier for use is their relative expense versus a card form factor. A Medicare CAC card would cost $24 per participant (full cost for implementation) whereas smart phone pricing begins at $200 per phone, with a two-year activation contract with a cell carrier. Not only would that cost be borne by the beneficiary, but not all beneficiaries can afford such an expense. Neilsen's third-quarter 2012 survey of mobile phone owners reports that less than 18% of seniors currently own a smart phone. As such, it would be an inappropriate form factor for Medicare CAC use now, and well into the foreseeable future.

**4. A paper from The National Health Law Program suggests that smart cards and biometrics can be a deterrent to care. How would a Medicare CAC smart card implementation impact seniors' access to healthcare including minority and low income communities?**

There would be no impact on senior's access to healthcare, even among minority and low income communities. The Medicare CAC card would be provided, free of charge, to all eligible seniors, just as the current Medicare card is. The Medicare CAC beneficiary card will utilize a four-digit PIN in order to authenticate the holder of the card is who they say they are, similar to bank cards used across the country. When sent to seniors, the PIN could be initially set to be the last four digits of the beneficiary's Social Security number, to aid in ease of use. Should the senior choose to change their PIN, they can do so easily when they see their healthcare provider using an authorized Medicare terminal.

In fact, Medicare CAC would bring enhanced protections to our nation's seniors, including minority and low-income communities. Currently, seniors' Social Security numbers are used as their Medicare identifier, and are printed directly on the front of their Medicare card. This poses a significant risk to seniors, as it puts them directly at risk for identity theft and fraud. Medicare CAC, however, would take the Social Security number off the front of the Medicare card and store it securely in the Medicare CAC's on-board computer chip, protected by strong encryption. Because of its beneficial impact on seniors, the American Association of Retired Persons (AARP) has endorsed the Medicare CAC Act.

**5. The Secure ID Coalition estimates that implementing a Medicare CAC smart card would reduce fraud by 50% within Medicare.**

*a. On what is this estimate based?*

As mentioned earlier in this document in response to Congressman Pitts' question #2 *(above)*, the Secure ID Coalition bases its 50% fraud reduction estimate on past implementations throughout the financial services and healthcare sectors, both throughout the U.S. and globally.

*b. How would identity theft be impacted by the implementation of a Medicare smart card?*

Across both the federal government and all 50 states, significant efforts have been made to move away from using the Social Security number (SSN) as an identifier for government services or for personal identification. In unfortunate contrast, the current Medicare card has seniors' SSN printed directly on the card, allowing any and all who may see it access to the number. Usually it is the only document in a senior's wallet that actually has their SSN printed on it, along with their name. Should it be stolen or unlawfully accessed, the senior's identity is at risk.

Further, when a beneficiary visits a provider's office, it is common practice for the office to take a photocopy of the Medicare card and place it in the beneficiary's file. This practice allows anyone with access to the files – medical billing staff, janitorial staff, and others – to surreptitiously glean this information for non-appropriate purposes.

Medicare CAC allows the SSN to be taken off of the front of the card and securely stored in the Medicare CAC's onboard computer. All information on the card is protected by strong encryption and can only be accessed by an authorized Medicare reader. Under no circumstances would the beneficiary's SSN ever be sent or viewed in an unencrypted manner or in the clear, further protecting the beneficiary's identity against theft or misappropriation.

*c. If implemented, how would the Medicare CAC pilot benefit providers and how could the challenges of implementation be mitigated?*

Medicare CAC would provide numerous benefits to providers; some of the benefits to doctors include:

<u>Quicker Processing of Payment</u>
Because transactions can be verified by both the provider and beneficiary a non-repeatable audit trail is created. Because the provider and beneficiary are tied together electronically using their smart cards paperwork is eliminated. Both of these reasons allow the provider to be paid within 48-72 hours.

<u>Billing Accuracy</u>
In many cases, claims are rejected because of small mistakes or typos. Because the chips verify both the provider and beneficiary all information is electronic, eliminating these types of mistakes.

<u>Eliminates the need for Recovery Audit Contractors (RACs)</u>
Because both beneficiaries and providers provide proof they are legitimate, payment is pre-approved before it is sent, eliminating the need for backend recovery audit contractors.

<u>Streamline Administrative Efficiency</u>

Smart cards store basic patient/beneficiary information on the secure chip. That information can be accessed by the provider at point of check-in to identify the correct patient and eliminate many of the administrative check-in procedures.

Protects Medicare Provider Numbers

Today provider numbers are widely available and used by thieves billing Medicare for products and services never performed. Using a smart card guarantees that no one can masquerade as the provider and use their number to bill Medicare.

Challenges to implementation would be mitigated by working directly with doctors and medical practice organizations to assist in the design and the streamlining of the Medicare CAC system. Discussions are currently underway with many such organizations.

d. ***In implementing any type of new Medicare card technology why are non-proprietary solutions and standards important and necessary?***

Building off of the answer to Congressman Pitts' question #7 *(above),* utilizing non-proprietary solutions and standards are important and necessary to creating a robust system, as well as allowing multiple vendors to bid to a known set of criteria, ensuring consistency of solutions and competitive pricing.

The open standards on which a smart card Medicare CAC system is based have been developed and vetted by the federal government as being strongly secure and highly protective of the information contained within. A proprietary system would face innumerable road-blocks in proving itself up to par with those standards for government use; smart cards have already crossed those hurdles and are being used across the federal government for a myriad of mission-critical applications that require security and reliability.

# SMART CARD ALLIANCE
# PROJECTED SCHEDULE OF COSTS
# TO DEPLOY SECURE ID CARD
# AND RELATED FRAUD REDUCTION COST
# SAVINGS AND RETURN ON INVESTMENT
# WITH
# INDEPENDENT ACCOUNTANTS' REPORT

DELEON & STANG
CERTIFIED PUBLIC ACCOUNTANTS AND ADVISORS

**DELEON & STANG**
CERTIFIED PUBLIC ACCOUNTANTS AND ADVISORS

100 Lakeforest Boulevard
Suite 650
Gaithersburg, MD 20877
P: 301-948-9825
F: 301-948-3220
www.deleonandstang.com

Allen P. DeLeon, CPA, P.C.
Richard C. Stang, CPA, P.C.
Jeanie Price

## INDEPENDENT ACCOUNTANTS' REPORT

**Smart Card Alliance**
**Washington, DC**

We have examined the accompanying projected Schedule of Costs to Deploy a Secure ID Card Within the U.S. Medicare System, and the Schedule of Projected and Fraud Reduction Cost Savings of Deployment of a Secure ID Card Within the U.S. Medicare System and the Related return on Investments (ROI) as of February 13, 2012, which has been prepared by Smart Card Alliance. Smart Card Alliance's management is responsible for the projections, which were prepared for the purpose of providing educational information relevant to proposed legislation being drafted by the U.S. Congress. Our responsibility is to express an opinion on the projections based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included such procedures as we considered necessary to evaluate both the assumptions used by management and the preparation and presentation of the projection. We believe that our examination provides a reasonable basis for our opinion.

In our opinion, the accompanying projections are presented in conformity with guidelines for presentation of a projection established by the American Institute of Certified Public Accountants, and the underlying assumptions provide a reasonable basis for management's projections assuming:

1. The deployment costs are accurately projected by using an average of the projected deployment costs based on a survey of six companies which specialize in deployment of similar secure ID cards for similar purposes in the U.S. and foreign countries, and other estimates of deployment costs made by the Smart Card Alliance, Health Council Members.
2. The quantity of projected users of the secure ID card are accurately estimated using U.S. Department of Health and Human Services (HHS) information as described in the projection.
3. The cost savings are accurately projected by using cost savings of similar programs in the U.S. and foreign countries, as described in the projection.
4. The return on investment (ROI) is accurately projected by using the projected cost savings and applying it to the estimated current levels of Medicare fraud.

However, even if the assumptions referred to above are accurate, there will usually be differences between the projected and actual results, because events and circumstances frequently do not occur as expected, and those differences may be material. We have no responsibility to update this report for events and circumstances occurring after the date of this report.

The accompanying projection and this report are intended solely for the information and use of (1) members of management of the Smart Card Alliance and (2) the U.S. Congress and related US government agencies, in connection with proposed legislation related to the deployment of secure ID cards, and are not intended to be and should not be used by anyone other than these specified parties.

*DeLeon & Stang*
**DeLeon & Stang, CPAs and Advisors**
**Gaithersburg, Maryland**
**June 27, 2012**

## SMART CARD ALLIANCE
## Schedule of Costs to Deploy a Secure ID Card Within the U. S. Medicare System
## February 13, 2012

**National Rollout**

| Professionals working at hospitals, physician's offices, Medical equipment suppliers, nursing homes, assisted living residences, mental health professionals and pharmacies who require ID cards. | Quantity | Source of information |
|---|---|---|
| **TOTAL PROFESSIONALS** | **2,624,884** | National Plan and provider Enumeration System Statistics 5/05 - 7/11 |

| Cards Required | Quantity | Price Per Unit | Total | |
|---|---|---|---|---|
| Professionals | 2,624,884 | $4.17 | $10,932,642 | See quantity above |
| Beneficiaries | 48,000,000 | $1.00 | $48,091,200 | Industry estimate |
| **TOTAL CARDS** | **50,624,884** | **$1.17** | **$59,023,842** | |

**Medicare Cost Summary**

| Providers and Suppliers | Users | Average Cost Per Person | Total | Comments |
|---|---|---|---|---|
| Enrollment of Providers and Suppliers | 2,624,884 | $12.82 | $33,637,888 | Cost to enroll everyone, prove licensing |
| Background Investigation (Vetting) | 2,624,884 | $0.00 | $0 | Already included in existing processing costs |
| Biometric AFIS Database | 2,624,884 | $0.59 | $1,557,869 | Checking against data base |
| Large Systems Integrator (LSI) | 2,624,884 | $0.76 | $1,994,912 | Allow cards to be read in existing CMS system |
| Digital Certificate - Level 3 MHW Assurance | 2,624,884 | $1.01 | $2,638,008 | Electronic version of ID recognition |
| Card Stock | 2,624,884 | $4.17 | $10,932,642 | Physical card from above |
| Card Issuance & Fulfillment | 2,624,884 | $3.25 | $8,522,123 | Mailing out cards |
| Card Manufacturer Professional Services | 2,624,884 | $0.10 | $262,488 | Consulting |
| Middleware/ Strong Authentication Server with Connect | 2,624,884 | $6.62 | $17,363,608 | Connect to software |
| Software Licensing | 2,624,884 | $1.25 | $3,283,730 | Licensing of vendor software |
| Card Management System (CMS) | 2,624,884 | $0.33 | $853,087 | Integration |
| Identity Management System (IDMS) | 2,624,884 | $0.21 | $538,101 | Integration |
| **PROVIDER & SUPPLIER TOTAL** | **2,624,884** | **$31.08** | **$81,584,457** | |

**SMART CARD ALLIANCE**
**Schedule of Costs to Deploy a Secure ID Card**
**Within the U. S. Medicare System**
**February 13, 2012 (Continued)**

| **Beneficiaries** | **Users** | **Per Person** | **Total** | |
|---|---|---|---|---|
| Digital Certificate plus Class 2 Identity Proofing | 48,000,000 | $2.82 | $135,200,000 | PIN required to activate |
| Card stock | 48,000,000 | $1.00 | $48,091,200 | Electronic version of ID recognition |
| Card Issuance & Fulfillment | 48,000,000 | $3.44 | $165,280,000 | Physical card from above |
| Card Manufacturer Professional Services | 48,000,000 | $0.07 | $3,120,000 | Mailing out cards |
| Middleware/ Strong Authentication Server with Connect | 48,000,000 | $0.23 | $11,040,000 | Consulting |
| Large Systems Integrator (LSI) | 48,000,000 | $5.24 | $251,520,000 | Connect to software |
| Software Licensing | 48,000,000 | $1.26 | $60,331,200 | Licensing of vendor software |
| Card Management System (CMS) | 48,000,000 | $0.32 | $15,120,000 | Integration |
| Identity Management System (IDMS) | 48,000,000 | $0.21 | $9,840,000 | Integration |
| **BENEFICIARY TOTAL** | **48,000,000** | **$14.57** | **$699,542,400** | |

| **Readers and Terminals** | **Quantity** | **Per Unit/Per Person** | **Total** | |
|---|---|---|---|---|
| USB Contact Readers | 170,537 | $7.50 | $1,279,025 | |
| Dual Slotted Terminals (German model) | 103,000 | $162.50 | $16,737,500 | |
| Biometric (Fingerprint) Readers | 170,537 | $80.00 | $13,642,933 | |
| | **444,073** | **$71.29** | **$31,659,458** | |
| **Activation Kiosks** | **17,500** | $23,666.61 | $414,165,675 | To change PIN, add photo, activate card |
| **GRAND TOTAL (National Rollout)** | **50,624,884** | **$24.24** | **$1,226,951,990** | |
| **Annual Maintenance of Total Cost** | 25% | | **$306,737,997.60** | % of total costs estimate |

**SMART CARD ALLIANCE**
**Schedule of Projected Fraud Reduction Cost Savings of**
**Deployment of a Secure ID Card in the U. S. Medicare System**
**And the Related Return on Investments**

| **Fraud** | | **Year 1** | **5 Yr. aggregate** | **10 yr. aggregate** |
|---|---|---|---|---|
| Current Situation | | $60,000,000,000 | $300,000,000,000 | $600,000,000,000 |
| **Fraud Reduction Percentage** | | **Savings** | | |
| | 10% | $6,000,000,000 | $30,000,000,000 | $60,000,000,000 |
| | 20% | $12,000,000,000 | $60,000,000,000 | $120,000,000,000 |
| | 33% | $19,800,000,000 | $99,000,000,000 | $198,000,000,000 |
| | 40% | $24,000,000,000 | $120,000,000,000 | $240,000,000,000 |
| | 50% | $30,000,000,000 | $150,000,000,000 | $300,000,000,000 |
| | 66% | $39,600,000,000 | $198,000,000,000 | $396,000,000,000 |
| | 70% | $42,000,000,000 | $210,000,000,000 | $420,000,000,000 |
| | 80% | $48,000,000,000 | $240,000,000,000 | $480,000,000,000 |
| | 90% | $54,000,000,000 | $270,000,000,000 | $540,000,000,000 |
| **Return on Investment** | | | | |
| **Fraud Reduced by** | | | | |
| | 10% | $4,466,310,012 | $27,239,358,022 | $55,705,668,034 |
| | 20% | $10,466,310,012 | $57,239,358,022 | $115,705,668,034 |
| | 33% | $18,266,310,012 | $96,239,358,022 | $193,705,668,034 |
| | 40% | $22,466,310,012 | $117,239,358,022 | $235,705,668,034 |
| | 50% | $28,466,310,012 | $147,239,358,022 | $295,705,668,034 |
| | 66% | $38,066,310,012 | $195,239,358,022 | $391,705,668,034 |
| | 70% | $40,466,310,012 | $207,239,358,022 | $415,705,668,034 |
| | 80% | $46,466,310,012 | $237,239,358,022 | $475,705,668,034 |
| | 90% | $52,466,310,012 | $267,239,358,022 | $535,705,668,034 |

**SMART CARD ALLIANCE**
**Project Deployment Costs and Fraud Reduction Savings of Secure ID Card**
**February 13, 2012**

## NOTE 1 - NATURE AND PURPOSE OF ORGANIZATION

The Smart Card Alliance is a non-profit organization, located in Washington DC and tax exempt under section 501 (c) (6) of the Internal Revenue Code (IRC). Its mission is to accelerate the widespread adoption, usage and application of smart card technology in North America, by bringing together users and technology providers in an open forum to address opportunities and challenges for the industry. Its membership consists of companies and individuals in technology companies, federal, state and local governments, academic institutions, consulting companies and Latin American companies and institutions. The Organization conducts conferences, prepares publications, and provides resources to its members in furtherance of its purpose.

## NOTE 2 - SPECIFIC PURPOSE OF THE PROJECTIONS

The purpose of this report is to provide projections related to (1) the estimated costs of the deployment of a secure ID card in the U.S. Medicare system to the U.S. Congress, (2) the estimated fraud reduction cost savings and return on investment (ROI), in relation to proposed legislation to conduct a pilot program.

## NOTE 3 - UNDERLYING ASSUMPTIONS USED ON THE PROJECTIONS

Certain assumptions were used in developing the projections. The projections are only as reliable as the accuracy of the assumptions. Even if the assumptions described in this report are accurate, there will usually be differences between projected results and actual results, because events and circumstances frequently do not occur as expected and those differences could be material. The underlying assumptions used to develop the projections in the report are:

1. The costs of deployment of a secure ID card are based on the average cost projections developed from a survey of technology companies which are members of the Smart Card Alliance. The survey consisted of six companies, and the projected costs are an average of the costs projected by these companies. Some companies did not provide cost information in all cost areas. Some of the estimates of deployment costs were made by the Smart Card Alliance and Healthcare Council Members, and not directly from the survey results. The surveyed companies; cost projections are only as accurate as the projections provided by the survey. Since the overall deployment costs are based on the cost per user multiplied by the number of projected users, the actual deployment costs could differ significantly from the projected costs if the actual cost per user is different from the projected cost per user.

**SMART CARD ALLIANCE**
**Project Deployment Costs and Fraud Reduction**
**Savings of Secure ID Card (Continued)**
**February 13, 2012**

**NOTE 3 - UNDERLYING ASSUMPTIONS USED ON THE PROJECTIONS** (Continued)

2. The quantity of projected users of the secure ID card was determined from information obtained from the National Plan and Provider Enumeration System (NPPES), a division of the Centers for Medicare and Medicaid Services (CMS) of the U. S. Department of Health and Human Services (HHS). Since the projected costs of deployment of a secure ID card is based on the cost per user multiplied by the number of projected users, the accuracy of the number of users is a material component in the total cost projection. The NPPES information is generally considered to the most current and accurate estimate of the number of users of a secure ID card. However, the overall deployment costs relies heavily on the quantity of users, and may differ significantly from the actual costs if the actual number of users differs from the projected number of users.
3. The fraud reduction cost savings is presented at various assumed percentages of savings. It is assumed that the current Medicare fraud is approximately $60 billion per year. The fraud reduction cost savings is based on cost savings of similar programs using other applications of the secure ID card and deployment of a secure ID card in other countries whose medical systems and related regulations differs from those in the U.S. While management believes that the fraud reduction cost savings reported by other secure card applications and deployments in other countries is a reasonable estimate of the fraud reduction cost savings that would be achieved in the U.S., material differences could exist which would affect the total cost savings.
4. The projected return on investment (ROI) is also presented at various assumed fraud reduction percentages. The projected ROI is computed by subtracting the total projected fraud cost savings, at each assumed savings percentages, from the projected deployment costs. Since the total projected deployment costs and the projected fraud reduction savings are based on the assumptions described above, the ROI is based on, and subject to, these assumptions. If the total projected deployment costs and/or the total projected cost savings differ materially from the actual results, the actual ROI will differ materially from the projected ROI.

## NOTE 4 - LIMITATIONS OF USE OF THE PROJECTIONS AND SPECIFIED PARTIES

The projected information contained in this report is intended for a specific purpose and use, it is not intended that the projections be used for any other purposes or uses. Further, this report is intended for use by (1) Members of the Smart Card Alliance, (2) the U.S. Congress and related U. S. government agencies related to proposed legislation concerning a pilot program for deployment of a secure ID card in the U.S. Medicare system, the use of this report is not intended to be used, and should not be used, by any other parties other than the specified users.

Responses of Michael H. Terzich
Senior Vice President of Global Sales & Marketing
Zebra Technologies Corporation

To the Honorable Joseph R. Pitts
Chairman, Subcommittee on Health
Committee on Energy & Commerce
U.S. House of Representatives

Regarding November 28, 2012 Hearing
"Examining Options to Combat Health Care Waste, Fraud and Abuse"

1. How will secure ID technology help reduce or eliminate fraud, waste and abuse in the Medicare system?

   ***Response***: Secure ID technology enjoys a strong record of performance in both the federal government and the private sector. The Department of Defense uses this technology as a federal government standard to secure logical and physical access to vital defense facilities. In the commercial world, global credit card companies use this kind of technology to protect the integrity of both personal identity and financial transactions. This experience leads us to believe that commercially available secure ID technology provides a tested platform that can be used in combating Medicare fraud, waste and abuse.

2. How will senior citizens be impacted by any possible transition from today's paper-based Medicare card format to a secure ID Medicare card format?

   ***Response***: The placement of a beneficiary's Social Security number on the front of the current Medicare card presents an identity theft hazard for seniors. By moving to a secure ID card format, the Social Security number is removed from plain sight and the additional protective measures that are part of secure ID technology will be available to ensure that seniors are safeguarded against fraud and identity theft.

3. Counterfeiting is a major challenge with identification. How does your company safeguard its secure card print technology so that counterfeiters cannot gain access?

   ***Response***: Counterfeiting secure cards is exponentially more difficult than counterfeiting paper-based cards, even for the most sophisticated, well-financed criminal enterprises. Supposing a criminal enterprise could gain access to a secure card printer, it would still have to reverse engineer the security system, obtain secure printing supplies, hack into the secure network, encode PIN or biometric data on the smart chip, print counterfeit cards and then use those cards to create fraudulent transactions – with all of that having to be done before the secure card printer was declared as missing. Even then, each fraudulent transaction would have a known identity which would speed the identification and investigation of subsequent transactions, making it more likely to capture the perpetrators quickly.

To ensure the printers produce only authorized credentials, printers can be programmed to respond only to print requests from specific host systems. These specially coded printers are made available only through secure channels. This secure distribution mechanism is in use today for secure card printers that print credit and debit cards on demand. Further, these card printers only accept ribbons and laminates specially tagged with secure RFID tags for those printers. To prevent any unauthorized access of these specially-coded ribbons, they are stored in secure vaults after encoding and delivered only through secure channels. Also, the printers can be locked after the ribbons and laminates are added so these printing supplies cannot be removed without proper authorization. Finally, the printers can be setup to print only when a security smart card is inserted by an authorized user.

4. What information, specifically, will be stored on the cards? Is beneficiary personal information vulnerable to unauthorized access by third parties?

***Response***: H.R. 2925, the Medicare Common Access Card Act introduced by Congressmen Shimkus and Gerlach in the 112th Congress, required the name and Social Security number to be stored on the card. The legislation provided discretion to the Secretary of HHS on whether to include additional information and test such possibilities in the five pilot projects. Since the legislation contemplated a contact-based system, personal information is protected against third party piracy. There's no power in a contact-based ID card until it comes in contact with a reader. This approach effectively requires the beneficiary to give affirmative consent to having their card read at the point of service delivery because the beneficiary must permit his or her card be inserted into a reader.

5. Has this kind of secure ID card technology been implemented in other health programs – either in the US or globally – and, if so, where has it been tried and what were the results?

***Response***: Many countries have implemented or are in the process of implementing smart cards for healthcare services. As examples, Taiwan and India have implemented secure ID technology for their healthcare programs:

- The Taiwan Healthcare Smart Card (Bureau of National Health Insurance card) program has been in existence since 2004. They have successfully issued over 23 million cards to all their citizens and some 300,000 to providers. These cards store personal information and medical history of the card holders in a secure, encrypted format. The medical history is accessible to healthcare providers only with the proper authorization from the card holders. Taiwan Bureau of National Health

Insurance card has reported dramatic reductions in medical costs from reduced fraud and more efficient claims processing.

- Rashtriya Swasthya Bima Yojna (RSBY) in India is a government-sponsored health insurance program for families below the poverty line. This program has been in existence since 2009 and is still being implemented across the country. So far, 34 million RSBY smart cards have been issued in India. These cards store biometric information of the beneficiaries in their smart chips. The program has received very positive reviews for ease of transactions both from program participants and service providers.

Domestically, we are aware of the efforts of individual hospitals and hospital systems across the country to employ secure ID card technology for a variety of purposes, including the improving the accuracy of the patient registration process, enhancing claims and payment processing accuracy, fraud prevention and the general savings that come from moving from labor-intensive, paper-based systems to more efficient digital systems. We understand that the Secure ID Coalition has detailed these points in its responses to the Subcommittee's questions and we associate ourselves with those responses.

6. Will the secure Medicare ID card format present challenges to older patients as the technology would require beneficiaries to remember a PIN number in order to use the card?

***Response***: Physicians already have processes in place for handling a transaction when a patient forgets his or her paper card today and similar procedures will continue to be needed in the future. Additionally, by moving more transactions to a secure status, there will be more time and human resources available to assist in such instances as well as in focusing on enhancing the overall integrity of the system.

7. You mentioned there is storage on the card, which for providers could carry biometric data. Could the card also carry electronic health records for the patients?

***Response***: There are many programs underway looking at Electronic Health Records and how those could be shared. It is **theoretically** possible to store them in a secure card but that is not necessary to start realizing the benefits of security and fraud prevention that are urgently needed today. The pilot program should move forward with these goals in mind.

8. Your testimony references the benefits of decentralized printing model rather than a centralized one. Please expand on the benefits and challenges associated with both a decentralized and a central print approach to creating secure Medicare ID cards.

***Response***: The advantages of a decentralized approach reflect the fact that security is enhanced when there is a concurrent, real-time tie between the creation of a secure ID card and the immediate, real-time verification of the cardholder's information. Delays or gaps in time between these two steps – which inevitably occur when cards are manufactured in a remote, centralized manner – increase opportunities for fraud which can be otherwise reduced or eliminated with the use of a decentralized print model.

9. Can you please provide to the committee a list of the fraud prevention areas that you believe could be improved within CMS? If these areas include deficiencies on the part of CMS, can you provide explanation as to why you believe those deficiencies exist? Can you also provide recommendations on ways that CMS fraud prevention can be improved?

***Response***: In general, Zebra associates itself with the Secure ID Coalition's original testimony and its corresponding responses to the Subcommittee's questions. In general, fraud prevention at CMS can be aided by a transition from the existing "pay-and-chase" system to a "fraud prevention" system. As outlined in the responses to previous questions, we believe the elements of a strong fraud prevention capability include the use of secure, digital card technology that will also help reduce the system operating costs of Medicare. In the case of secure ID cards, we reiterate our view that both security and efficiency are substantially enhanced through the use of a decentralized print model which provides a real-time tie between the creation of a secure ID card and the immediate verification of the cardholder's information. Delays or gaps in time between these two steps – which inevitably occur when cards are manufactured in a remote, centralized manner – increase opportunities for fraud that can be otherwise reduced through the use of a decentralized print model.

○