S. Hrg. 112–310

HARNESSING TECHNOLOGY AND INNOVATION TO CUT WASTE AND CURB FRAUD IN FEDERAL HEALTH PROGRAMS

HEARING

BEFORE THE

FEDERAL FINANCIAL MANAGEMENT, GOVERNMENT INFORMATION, FEDERAL SERVICES, AND INTERNATIONAL SECURITY SUBCOMMITTEE

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

JULY 12, 2011

Available via the World Wide Web: http://www.fdsys.gov

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

68–015 PDF WASHINGTON : 2012

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 HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
THOMAS R. CARPER, Delaware
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana
CLAIRE MCCASKILL, Missouri
JON TESTER, Montana
MARK BEGICH, Alaska

SUSAN M. COLLINS, Maine
TOM COBURN, Oklahoma
SCOTT P. BROWN, Massachusetts
JOHN MCCAIN, Arizona
RON JOHNSON, Wisconsin
ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JERRY MORAN, Kansas

MICHAEL L. ALEXANDER, *Staff Director*
NICHOLAS A. ROSSI, *Minority Staff Director*
TRINA DRIESSNACK TYRER, *Chief Clerk*
JOYCE WARD, *Publications Clerk and GPO Detailee*

SUBCOMMITTEE ON FEDERAL FINANCIAL MANAGEMENT, GOVERNMENT INFORMATION, FEDERAL SERVICES, AND INTERNATIONAL SECURITY

THOMAS R. CARPER, Delaware, *Chairman*

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
MARK L. PRYOR, Arkansas
CLAIRE MCCASKILL, Missouri
MARK BEGICH, Alaska

SCOTT P. BROWN, Massachusetts
TOM COBURN, Oklahoma
JOHN MCCAIN, Arizona
RON JOHNSON, Wisconsin
ROB PORTMAN, Ohio

JOHN KILVINGTON, *Staff Director*
WILLIAM WRIGHT, *Minority Staff Director*
DEIRDRE G. ARMSTRONG, *Chief Clerk*

CONTENTS

WITNESSES

TUESDAY, JULY 12, 2011

ALPHABETICAL LIST OF WITNESSES

APPENDIX

HARNESSING TECHNOLOGY AND INNOVATION TO CUT WASTE AND CURB FRAUD IN FEDERAL HEALTH PROGRAMS

TUESDAY, JULY 12, 2011

U.S. SENATE,
SUBCOMMITTEE ON FEDERAL FINANCIAL MANAGEMENT,
GOVERNMENT INFORMATION, FEDERAL SERVICES,
AND INTERNATIONAL SECURITY,
OF THE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:34 p.m., in room 342, Dirksen Senate Office Building, Hon. Thomas R. Carper, Chairman of the Subcommittee, presiding.

Present: Senators Carper, McCaskill, Brown, and Coburn.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Well, why don't we go ahead and invite our first panel to the table, please. Welcome, one and all.

On most Tuesdays that we are in session, Senate Democrats and Senate Republicans eat lunch, never together, always apart, and talk about the challenges that we face as a Nation, and we spent the last hour, hour-and-a-half in the Senate Democratic Caucus talking about the budgetary challenges that we face and what to do about them. One of the people who has thought about this for a lot longer than this week or this month or this year is the fellow who is sitting to my right, Senator Coburn, who has just joined us.

He was a member of a commission created by Executive Order (EO) by the President over a year ago called the Deficit Commission, co-chaired by Erskine Bowles and by former Senator Alan Simpson, and 11 of the 18 members of that Commission voted for a deficit reduction package that would basically reduce the deficits by about $4 trillion over the next 10 years, mostly on the spending side, some on the revenue side. It was an approach in which almost everything was on the table—defense spending, domestic discretionary spending, entitlement spending, tax expenditures, and weighted about two-to-one or three-to-one to the spending side in terms of deficit reduction.

One of the concerns, primarily among Democrats but also by Republicans and some Independents, is how do we reduce entitlement spending without significantly cutting benefits and inflicting real harm on people. Thanks to the good work by folks on my staff and on Senator Coburn's staff, some good work has been done drilling

down on Medicare and on Medicaid to find there are ways for us to be able to reduce outlays from those programs, but to do so in a way that does not mortally wound beneficiaries or, frankly, mortally wound the providers.

As it turns out, there is a lot that we can do and there is a fair amount that we are doing. The health care legislation that we passed here a year or so ago actually provides a number of tools to the Centers for Medicare and Medicaid Services (CMS) to enable them to go out and save some money and to reduce the flight of funds, almost the thievery of funds, the theft of funds from the Medicare Trust Fund.

Senator Coburn and I have been working, and our staffs have been working to see if there are other things that we can do to shore up the Medicare Trust Fund, which is now scheduled to run out of money in 2024. As it turns out, there is a fair amount that we can do in our role to help some of you at this table, especially Dr. Budetti and his folks, to realize additional savings. And a lot of us would just say it is common sense.

The fellow who just handed me my talking points here is Peter Tyler. Peter has done great work here along with the Republican staff. But one of the things that we learned most recently was that in 2007, if you look at the amount of money that was spent—what was the expenditure, Peter, what was it for 2007? About half of what was spent on power wheelchairs. I do not know if this came from the Inspector General (IG) or from the Government Accountability Office (GAO) or who. Who did it come from, the IG?

Dr. BUDETTI. The Office of Inspector General (OIG).

Senator CARPER. Yes, the IG. In the first half of 2007, we spent, I think, about $190 million for power wheelchairs that year, and roughly half of that was, frankly, pretty hard to prove it should have been spent.

We have dead doctors writing prescriptions for controlled substances for folks who should not be receiving those substances. They are going out and filling those prescriptions and using the drugs to help feed the drug trade. It is far too easy for bad people, for folks with criminal intent to get their hands on the provider IDs, and they are not only ordering controlled substances, but all kinds of durable medical equipment (DME). There is just a lot going on.

You look at improper payments, $125 billion, I think GAO tells us, last year, about $47 billion of that for Medicare, not counting the Medicare Prescription Drug Program. I am told there is about another 20 or so billion dollars last year for Medicaid improper payments. Eric Holder, our Attorney General, tells us there is $60 billion in Medicare fraud. I do not know if he is combining some of those numbers out of improper payments or not, but it is a lot of money. And if the President says we are going to cut improper payments in Medicare by half by the end of next year, if we do that, that is $25 billion a year. If you do it for 10 years, that is $250 billion. That is a quarter-of-a-trillion. If we take out half of the fraud in Medicare, that is another $30 billion a year times 10 years is $300 billion. And you add it together and we are talking about real money, and none of that has to savage beneficiaries or inconvenience providers.

We are interested in getting better results for less money, and we have been interested in that in health care. We are interested in a lot of other ways. And one of the ways to do that is to, frankly, drill down into some of the stuff we are going to talk about today.

I am just very grateful to each of the witnesses for coming, for preparing for today's hearing, and with that, I am going to yield to Senator Brown. Thanks very much.

OPENING STATEMENT OF SENATOR BROWN

Senator BROWN. Thank you, Mr. Chairman. It is good to see you again.

Senator CARPER. Nice to see you.

Senator BROWN. We are beginning to face difficult decisions that must be made in order to put our Nation back on the path to economic prosperity and fiscal sustainability, and one step we can all agree on is eliminating the waste, fraud, and abuse. Senator Coburn and Senator Carper were working on it long before I did. It is about $100 billion a year, and that is why I joined both of them in supporting the "FAST" Act of 2011, as one of the early cosponsors. It is a crucial tool for the government to attack this monumental waste of taxpayer dollars.

This is the second hearing in 5 months that this Subcommittee has held, finding out ways to root out waste and abuse in the system. It is the key to ensuring the viability for these important programs. Simply put, it is no longer acceptable, for business as usual, approach and the endless promises for action while the problem of waste, fraud and abuse continues to grow. This legislation is important and is long overdue.

As I stated at the Subcommittee's March 9 hearing, the Patient Protection and Affordable Care Act (PPACA) expands Medicaid coverage by an estimated 16 million people by 2019. That is a 32 percent increase over the current enrollment in the program, and the cost of the Medicaid expansion alone is estimated to be about $430 billion over the next 10 years, and the Federal Government is responsible for paying over 90 percent of these increases.

This expansion in the government's role in health care will unduly strain our Nation's already dire fiscal condition and entice predators that you referenced, Mr. Chairman, just now, to gorge on the cash cow which these programs represent. It is the government's chronic mismanagement of Medicare and Medicaid fraud prevention that has landed both programs on the GAO's High-Risk List for many years. Expanding benefits without first establishing the necessary controls, checks, and balances to prevent the waste, fraud, and abuse we all hear about is putting the cart before the horse.

The government's performance overseeing these programs in the last few decades does not indicate a history of success, and in light of the burgeoning wave of health care spending and the history of lax oversight, we need to do more and we need to do it quickly.

Today, we will hear about CMS's progress in confronting these areas through efforts like creation of the Integrated Data Repository (IDR) program. The IDR was created to provide a single source of data related to Medicare and Medicaid claims, a good first step. They began incorporating data in 2006, but have yet to incorporate

any Medicaid data. At the behest of Congress, CMS recently began the use of predictive modeling software to prevent payment of possible fraudulent claims. This has historically been at the heart of the problem, is trying to identify a lot of these fraudulent claims, and Congress has that oversight duty through your leadership, Mr. Chairman, to be proactive in pursuing ways to obtain—to curb that waste, fraud, and abuse.

So we have a lot of work to do. The American taxpayers expect more. We expect more and we need to move quickly, so I appreciate you holding this hearing.

Senator CARPER. Thanks, and I am happy to be here with you.

Senator Coburn, and I again just want to say thanks for letting me be your wingman on some of this stuff, improper payments——

Senator COBURN. I think you have said it all. I will look forward to hearing testimony.

Senator CARPER. All right. Great. Thanks so much.

All right. Let me give some brief introductions for our witnesses. Dr. Budetti, I am glad we are not paying you on an appearance basis because this could get expensive, but our first witness today is Dr. Peter Budetti. He is the Deputy Administrator and Director for Program at the Centers for Medicare and Medicaid Services. He is, in effect, the person in charge of combating waste and fraud for both the Medicare and the Medicaid programs—no small job. Dr. Budetti has a long history in the health care arena in both government and private sector, including Chairman of the Board of Directors at Taxpayers Against Fraud and as a professor at the University of Oklahoma. Dr. Budetti generously testifies in front of our Subcommittee quite frequently and we thank you very much for being with us today.

Lewis Morris, also known as Lew Morris, right?

Mr. MORRIS. Yes, sir.

Senator CARPER. There you go. He is the Chief Counsel of the Department of Health and Human Services (HHS), Office of Inspector General. Mr. Morris has worked for 25 years for the Inspector General. He has also served as Special Assistant U.S. Attorney for the Middle District of Florida, the Eastern District of Pennsylvania, and the District of Columbia. He also serves on the Board of Directors of the American Health Lawyers Association, and Mr. Morris, it is good to see you and thanks so much for your testimony and your preparation for today.

Joe Willemssen, who joins us today from the Government Accountability Office, is the Managing Director of the Government Accountability Office's Information Technology Team, where he oversees evaluations of technology across the Federal Government. This includes assessments of computer security, electronic government, privacy and systems acquisition. He has been at GAO for over 30 years, and I understand he has testified more than 80 times before Congress. Mr. Willemssen received both a Bachelor's and Master's degree in business administration from the University of Iowa. I think that makes you a Hawkeye for life. We are glad that you are here with us today.

And we finally want to welcome Louis—do people call you Lou or Louis?

Mr. SACCOCCIO. Lou.

Senator CARPER. Lou Saccoccio, who is Executive Director at the National Health Care Anti-Fraud Association (NHCAA), a national organization focused exclusively on combating health care fraud in both the public and the private sectors. We focus a lot on the public, fraud in the public sector, but it turns out there is a lot in the private sectors, as well, and we can learn from them. Maybe they can learn something from us. Mr. Saccoccio has served as Executive Director for over 6 years. Previously, he worked at the organization America's Health Insurance Plans. He is a graduate of the U.S. Naval Academy—Bravo Zulu—and also of Harvard Law School, and he served as a Navy JAG lawyer.

Mr. Saccoccio, always glad to have another Navy guy.

You have a common bond with at least two of us, maybe three, I do not know, but we are happy to have you.

Each of you have roughly 5 minutes to make your statement. If you go a little bit over that, that is OK. If you go way over it, that is not OK. I will rein you in. So I would just ask you to go ahead and your full statements will be made part of the record.

So, Dr. Budetti, please proceed. Thank you all, again, for joining us.

STATEMENT OF PETER BUDETTI, M.D.,[1] DEPUTY ADMINISTRATOR AND DIRECTOR FOR PROGRAM INTEGRITY, CENTERS FOR MEDICARE AND MEDICAID SERVICES

Dr. BUDETTI. Thank you, Senator Carper, Ranking Member Brown, and Senator Coburn. Good to be here again. It is my pleasure to be here before the Subcommittee and have the chance to tell you that there actually is some good news, that on July 1 of this year we at CMS implemented a new predictive modeling technology that was developed with private industry experts to fight Medicare fraud.

This is built on technology that has been used in the private sector and it will help identify fraudulent Medicare claims prior to their being paid on a nationwide basis so that we can begin to take action to stop fraudulent payments before they are made. This, of course, builds on the anti-fraud tools that we were provided in the Affordable Care Act (ACA), including enhanced screening and enrollment requirements, strengthened authority to suspend payments pending credible allegations of fraud and increased coordination of anti-fraud actions and policies across Medicare and Medicaid. This is helping us move from beyond the pay-and-chase mode into a new era of preventing problems prior to payment.

You have all seen my poster before. I just want to use it once again to highlight the top three lines. First of all, that we are moving to a prevention mode. Second, that we are targeting our resources based on the actual risk that we are facing. And third, that we are moving to use innovative and advanced technologies that have not previously been used in this fight against fraud.

I would like to now move on to telling you about our predictive modeling system that we have put into place, and I am pleased to be able to bring you up to date on this. This is not easy to do, but it is a challenge that we take on willingly. The Administration is

[1] The prepared statement of Mr. Budetti appears in the appendix on page 43.

committed to this action and we are going to move forward with it very enthusiastically.

The main purpose of this slide is to confuse you.

Senator CARPER. So far, it is working. [Laughter.]

Dr. BUDETTI. It is to illustrate how the new system will integrate into the claims payment system. You all know that claims go into our Medicare Administrative Contractors (MACs). They also then go through a series of other steps, and our fraud prevention system will intervene in the claims payment cycle. So this is not going to interfere with the claims payment process unless and until there is a reason to stop a claim from being paid, and I will be delighted to talk more about that in just a few minutes.

The result of the analysis will be fraud alerts, risk alerts that will tell us that we need to look more carefully at individual or patterns of claims, and we will use that information to target our investigative resources. This will lead to administrative actions by CMS. It will also lead to referrals to our law enforcement partners.

So this is an important step forward. It is a new system and it has been in place now for exactly 12 days. The system uses algorithms and advanced data analytics to look at many different factors, all simultaneously. Another characteristic of the system is that it is capable of and will, in fact, grow over time. As we get more experience with it, as we know which of our analyses are, in fact, paying off with fraud leads that are worth pursuing, that will then feed back into the system. As we learn from our law enforcement colleagues information from their investigations and other work, patterns that we should incorporate into our system, the system can incorporate that, as well. We can look at information by beneficiary, by provider, by service origin, by a variety of different approaches, all simultaneously.

We are also moving to deal with the information that is generated by the system in a number of ways. We are setting up a command center that will look at the alerts, will prioritize them, will triage them, and will take appropriate action very quickly, whether that is referral to our program integrity anti-fraud contractors to do investigations, whether it is immediate action by us, whether it is immediate referral to law enforcement.

We are also going to be prioritizing our vulnerabilities, looking more carefully at exactly what the vulnerabilities are that need to be expanded in the fraud prevention system that we are implementing.

And we are building a sandbox, an analytics sandbox that will include data from many sources, including the Integrated Data Repository and other sources of information. This will allow us to test additional models and additional algorithms and incorporate the ones that are likely to pay off into the system.

I want to emphasize that this system is one that was used in the private sector and it was immediately applicable to the Medicare system. So we were able to implement it just within 9 months of when the President signed the bill and within the statutory deadline that you provided us with.

I look forward to continuing to tell you about this and I look forward to your support and working with you as we move forward to fight fraud in health care. Thank you.

Senator CARPER. Well, good. Thanks for that opening statement. We will look forward to pursuing a number of points that you have raised. That is good. Thanks.

Mr. Morris, please proceed. Again, welcome. We appreciate the great work that you and your team have done.

STATEMENT OF LEWIS MORRIS,[1] CHIEF COUNSEL, OFFICE OF INSPECTOR GENERAL, U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Mr. MORRIS. Thank you very much. Chairman Carper, Ranking Member Brown, and Senator Coburn, thank you for the opportunity to testify this afternoon about the role that technology can play in cutting waste and fraud in the Federal health care programs.

The Office of Inspector General's anti-fraud efforts are substantially enhanced by information technology (IT). Data mining and analytics help us conduct risk assessments, target our oversight efforts, and reduce the time and resources required for audits, investigations, and other program integrity activities. By integrating data from Medicare Parts A, B, and D into a data warehouse and harnessing powerful analytic tools, we have expanded our analysis of questionable billing practices.

For example, through data mining and analytics, we found that Medicare was spending about $4,400 per beneficiary for inhalation drugs in South Florida compared to $815 for the beneficiaries in the rest of the country. By combining the drug manufacturers' sale data and Medicare claims information for a particularly expensive inhalation drug, we discovered that South Florida suppliers billed Medicare 17 times more units of the drug than was actually distributed for sale in that region.

Thanks to increased data storage and analytic capabilities, we are now more efficiently identifying providers that present compliance risks. For example, we are using data mining techniques to construct a comprehensive picture of a hospital's billing vulnerabilities. Two years ago, the analysis would have taken weeks or months to execute. Now, it takes approximately 20 minutes to run the computer program for each hospital.

Senator CARPER. Say that one more time.

Mr. MORRIS. What took us months 2 years ago to construct the actual software package and apply it to a hospital's set of compliance issues, we can now do in about 20 minutes. We have started a series of audits already looking at up to 28 different risk areas in a hospital system by pulling samples of claims and then going back to that hospital, identifying those compliance issues, and allowing them to not only repay the money owed to our program, but take a much closer look at their internal controls so that when we come back in a year or two, we hope to have found corrective action so we do not need to keep repeating the pay and chase.

Senator CARPER. Good. Thank you.

Mr. MORRIS. As exemplified by the Medicare Fraud Strike Force data, it is combined with field intelligence to enable us to identify fraud schemes and trends more quickly. This data-driven approach

[1] The prepared statement of Mr. Morris appears in the appendix on page 55.

pinpoints fraud hot spots, identifies suspicious billing patterns, and targets criminal behavior as it occurs. The Strike Force model has proven highly successful and has accelerated the government's response to health care fraud, decreasing by half the average time from an investigator's start to the prosecution in these types of cases. Since their inception in 2007, Strike Force teams have charged over 1,000 individuals with attempting to defraud Medicare of over $2.4 billion.

We also recognize that we can learn a great deal from the private health care insurers, who have developed technological expertise in addressing our common goal of stopping health care fraud. It is axiomatic that most criminals who prey on the Nation's health care system are equal opportunity thieves. They defraud private health care insurance as well as the Federal health care programs.

OI agents actively participate in health care fraud working groups, which bring together government agencies and private sector insurers to share field intelligence and ongoing schemes and develop best practices. We also conduct joint investigations with the private sector.

While the use of technology allows for a more efficient and targeted approach, several caveats are in order. First, human intelligence remains a key part of any program integrity strategy. Medicine and the health care system are extremely complex. A data run, even if derived from sophisticated metrics and powerful computers, cannot replace the role of professionals who bring experience and insight into the analysis of that data.

In addition, while predictive analytics have proven effective in identifying potential fraud in the credit card transactions, there are characteristics of the Federal health care program that may limit the usefulness of these tools in the health care environment. For example, a treatment that may be medically unnecessary but may not be apparent on the face of the claim for reimbursement.

It is also important to recognize that fraud schemes will evolve in response to these technologies, which introduce new vulnerabilities. For example, electronic health records (EHR) may not only facilitate more accurate billing and increase quality of care, but these electronic health records may also facilitate fraudulent claims. The very aspects of these records that make a physician's job easier-—cut and paste features and templates—can also be used to fabricate information that results in improper payments and leads to inaccurate and potentially dangerous information on a patient's record.

A final caveat. Even the best anti-fraud technology are of limited value if not effectively implemented and appropriately overseen. The OIG work spanning a decade has revealed persistent problems with the performance of CMS's program integrity contractors and vulnerabilities in CMS's oversight. Because CMS is relying on contractors to perform these data-driven program integrity functions, there is a critical need for meaningful performance evaluation and adequate oversight of that work.

In summary, technology can be a powerful weapon in the fight against fraud, but it is not a silver bullet. We must be mindful to carefully implement and oversee its use, and I would be pleased to answer any questions.

Senator CARPER. Great. Thanks so much, Mr. Morris.
Mr. Willemssen, please proceed.

STATEMENT OF JOEL C. WILLEMSSEN,[1] MANAGING DIRECTOR, INFORMATION TECHNOLOGY ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WILLEMSSEN. Thank you, Mr. Chairman, Ranking Member Brown, Senator Coburn. Thank you for inviting us to testify today on your hearing on Medicare and practices to reduce fraud and waste in Medicare and Medicaid.

At your request, we produced a report that is being released today on two CMS programs intended to improve the ability to detect waste, fraud, and abuse. As requested, I will briefly summarize our statement, which is based on that report, and I will also say that we have not looked at the initiative that Dr. Budetti discussed, but it sounds intriguing. We are interested to hear more.

But in talking about our statement today, I will briefly touch on three areas. One, discuss the extent to which the Integrated Data Repository and One Program Integrity (One PI), have been developed and implemented. Two, address CMS efforts to identify, measure, and track benefits resulting from those programs. And finally, I will talk about the recommendations we have made to CMS to help achieve its goals of reducing fraud, waste, and abuse.

Regarding IDR, it has been in use since 2006 and it is a very large data warehouse that can be of great benefit to CMS. However, currently, it does not include all the data that were planned to be in it by 2010. For example, IDR currently includes most types of Medicare claims data but not Medicaid data. IDR also does not include data from other CMS systems that can help analysts prevent improper payments. Further, CMS has not finalized plans or developed reliable schedules for efforts to incorporate these data.

One PI is a web-based portal that is to provide CMS staff and contractors with a single source of access to the data contained in IDR as well as tools for analyzing those data. While One PI has been developed and deployed, we found that few analysts were trained in using the system. Program officials planned for 639 analysts to be using the system by the end of Fiscal Year 2010. However, as of October 2010, only 41 were actively using the portal and tools. Until program officials finalize plans and schedules for training and expanding the use of One PI, the agency may continue to experience delays.

With One PI, CMS anticipated that it would achieve financial benefits of $21 billion. As we have previously reported, agencies should forecast expected benefits and then measure the actual results accrued through the implementation of programs. However, CMS is not yet positioned to do this. As a result, it is unknown whether the program has provided any financial benefits yet. CMS officials added it is too early to determine whether the program has provided benefits since it has not yet met its goals for widespread use.

To help ensure that the development and implementation of IDR and One PI are successful in helping CMS meet the goals of its

[1] The prepared statement of Mr. Willemssen appears in the appendix on page 66.

program integrity initiatives and possibly save tens of billions of dollars, we are making several recommendations to CMS. Among those, one, to finalize plans and schedules for incorporating additional data into the data repository. Two, finalize plans and schedules for training all program integrity analysts intended to use One PI. Three, establish and communicate deadlines for program integrity contractors to complete training and use of One PI. And four, to establish and track measurable outcome-based performance measures that gauge progress toward meeting program goals.

In commenting on a draft of our report, CMS agreed with our recommendations. CMS's timely implementation of these could lead to reduced fraud and waste and overall substantial savings in the Medicare and Medicaid programs.

That concludes a summary of my statement. I look forward to your questions. Thank you.

Senator CARPER. Thanks, Mr. Willemssen. Thank you so much. Mr. Saccoccio, please proceed.

STATEMENT OF LOUIS SACCOCCIO,[1] EXECUTIVE DIRECTOR, NATIONAL HEALTH CARE ANTI-FRAUD ASSOCIATION

Mr. SACCOCCIO. Thank you. Chairman Carper, Ranking Member Brown, and Senator Coburn, thank you for the opportunity this afternoon to testify.

The National Health Care Anti-Fraud Association was established in 1985 and is the leading national organization focused exclusively on combating health care fraud. We are uncommon among associations in that we are a private-public partnership. Our members comprise more than 85 of the Nation's most prominent private health insurers along with more than 85 Federal, State, and local government, law enforcement, and regulatory agencies that have jurisdiction over health care fraud who participate in NHCAA's law enforcement liaisons.

NHCAA's mission is simple: 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. The magnitude of this mission remains the same regardless of whether a patient has health coverage as an individual or through an employer or has coverage under a public program, such as Medicare, Medicaid, or TRICARE.

Health care fraud is a serious and costly problem that affects every patient and every taxpayer in America. Just as importantly, health care fraud is a crime that directly affects the quality of health care delivery. Patients are physically and emotionally harmed by health care fraud. As a result, fighting health care fraud is not just a financial necessity, it is a patient safety imperative.

Health care fraud does not discriminate also between types of medical coverage. The same schemes used to defraud Medicare mitigate over to private insurers and schemes perpetrated against private insurers make their way into government programs. Additionally, many private insurers are Medicare Part C and D contractors that provide Medicare coverage and Medicaid coverage in the

[1] The prepared statement of Mr. Saccoccio appears in the appendix on page 79.

States, making clear the intrinsic connection between private and public interest.

As a result, the main point I want to emphasize is the importance of anti-fraud cooperation and collaboration between private and public payers. NHCAA has stood as an example of the power of a private-public partnership against health care fraud since its founding, and we believe that health care fraud should be addressed with private-public solutions.

One salient example that illustrates the power of cooperative efforts against health care fraud can be found in South Florida. In response to the challenge of health care fraud schemes in South Florida, including fraud schemes involving infusion therapy and home health care, NHCAA formed the South Florida Work Group. In meetings held in 2009 and 2010, this NHCAA work group brought together representatives of private insurers, FBI headquarters and 10 FBI field divisions, CMS, HHS's Office of Inspector General, the Justice Department, the Miami U.S. Attorney's Office, and local law enforcement to address the health care fraud schemes emerging from South Florida. The details of the emerging schemes, investigatory tactics, and the results of recent prosecutions were discussed with the dual goals of preventing additional losses in South Florida and preventing the schemes from spreading and taking hold in other parts of the Nation.

This type of anti-fraud information sharing, sharing between the Federal and State programs and between private and public payers, is critical to the success of anti-fraud efforts. The HHS Office of Inspector General, CMS, the FBI, and the Justice Department have demonstrated a strong commitment to information sharing and are working with NHCAA to identify the barriers, both actual and perceived, to effective anti-fraud information sharing with the goal of increasing the effectiveness of this critical tool in the fight against health care fraud.

In addition to information sharing, the other critical means needed to detect and identify emerging fraud patterns and schemes in a timely manner is to apply effective and cutting-edge data analytics to aggregated claims data. 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.

In this regard, we applaud CMS for its recent implementation of predictive modeling using rules and pattern recognition for Medicare claims. NHCAA is also encouraged by the expanded provisions provided in the Affordable Care Act. The Act mandates an expanded integrated data repository that will incorporate data from all Federal health care programs.

Progress is also being made by commercial health insurers. In addition to the business rules and outlier models used by insurers to detect potential fraud, some companies have begun to utilize or are in the process of evaluating the use of predictive modeling technology and other advanced data analytics, applying them to fraud prevention efforts on the front end prior to medical claims being paid. Although the health care industry has not achieved the level of real-time data analytics used in the financial services industry, it is moving in the right direction.

NHCAA is encouraged by the renewed Federal emphasis given to fighting health care fraud. We know continued investment and innovation are critical, and as greater attention is given to eradicating fraud from our government health care programs, we urge decisionmakers to also recognize and encourage the important role that private insurers play in minimizing fraud in our Nation's health care system.

Thank you for allowing me to speak today. I will certainly answer any questions from you.

Senator CARPER. Thanks for that testimony. I thought your testimony was just excellent and enjoyed reading it and hearing it in here today. Thanks.

Let me start, if I could, with Dr. Budetti. First, I would like to address an issue that has been raised by GAO. First, before I do that, I just want to say, Dr. Budetti, that the Office of Program Integrity under your leadership has made, I think, a lot of progress, and there are a number of people responsible for that, but I just want to say to you, thank you. Since you took your position last year, there have been any number of positive efforts underway, including the implementation of program integrity provisions within the Affordable Care Act. I think you deserve a lot of credit. So does your team, as do many of your colleagues at the Center for Medicare and Medicaid Services.

However, as I say oftentimes in this room, everything I do, I know I can do better. The same is true for all of us, and the enormous waste and fraud challenges that we have, that we have heard about again here today, we have heard about in the past and, hopefully, we will hear about in smaller magnitudes in the future. But those challenges call out for very large efforts and require that the Congress ensures that the Federal Government takes many more strides to cut back on waste and fraud and abuse where we can.

Now, in the GAO testimony and their audit report released today, the fraud detection system, that is the combined Integrated Data Repository and One PI, is presented as an important new tool to examine Medicare and Medicaid payments in order to detect fraud, and it is depicted on this chart[1] up to my left and to your right. In fact, the Centers for Medicare and Medicaid Services own estimates show that if it is fully implemented, the new fraud detection systems will save some $21 billion—$21 billion—over 10 years by detecting and avoiding improper payments. The cost to date for the system is about $161 million, and to complete and operate the system for 10 years, the additional cost is roughly $184 million.

That is quite a return on investment (ROI), if you think about it, and curbing $21 billion in waste and fraud would represent a lot of progress—a lot more progress. I think it makes sense that the timely implementation would help get these cost savings, obtain these cost savings more rapidly. That is what we want to do.

However, the GAO has clearly shown that the system is not fully deployed. Despite the Centers for Medicare and Medicaid Services declaring the system up and running, only, as we have heard, 42 people were trained in 2010, and despite the stated requirement for, I think, 639 people. Further, the system has yet to include

[1] The chart referenced by Senator Carper appears in the appendix on page 118.

Medicaid data. Also, GAO reported that there are no clear plans nor projected dates with specific milestones to either train more people nor to include the Medicaid data. And despite being part of the original design, there are no solid plans to give access to Medicaid State offices, I am told.

Obviously, without the system being fully implemented as well as ensuring that Federal staff, oversight contractors, and law enforcement have access and are fully engaged, we will not realize that $21 billion in savings and that would be a shame.

So, Dr. Budetti, let me just ask, what is your plan schedule to fully implement and deploy the new fraud detection system? When will we have more people trained? And when will State Medicaid offices have access to this system?

Dr. BUDETTI. Thank you very much for your comments, Senator. I want to add that we always welcome the kind of arms' length oversight that we receive from the General Accounting Office—the Government Accountability Office—I dated myself there—and from our colleagues at the Office of Inspector General. And, in this case, we do, in fact, concur with their recommendations.

Senator CARPER. Can I just make a comment?

Dr. BUDETTI. Certainly.

Senator CARPER. I say this a lot. We are all in this together.

Dr. BUDETTI. Yes.

Senator CARPER. We are all in this together. And the only way for us to get out of this hole, this fiscal hole that we are in, including some that we are talking about here, is to get out together. Go ahead.

Dr. BUDETTI. And we very much appreciate the interest and support you have shown in this.

The Integrated Data Repository and the One PI system are ones that were started some 5 years ago or so. The agency did set rather ambitious goals for itself in terms of the implementation of those and some of those goals have been met. Some of them have not been met. This illustrates a number of factors. First of all, it does illustrate to some degree the challenges of implementing systems, especially, for example, with respect to the Medicaid data because States have different kinds of data systems and different formats and different responsibilities on the States in terms of their ability to supply the data. The structure of the Integrated Data Repository at first had to be, as I understand it, had to be redone somewhat. So there were some problems along the line in terms of meeting certain deadlines. Others were met.

But in terms of your specific questions, I would like to make a couple of points, sir. One is that the Integrated Data Repository is intended for many purposes other than just fighting fraud. It is a valuable resource and it still continues to be a valuable resource and it will be as we move forward with our new and advanced technological solutions that I mentioned earlier. But the Integrated Data Repository is not strictly for that purpose. It also has a variety of other uses within CMS and that is an important aspect of this.

The other question that you asked about, the training, we have, in fact, now trained an additional 55 personnel so far this year. We now have a schedule for training all of the private sector personnel

who are going to be working with the One PI and Integrated Data Repository——

Senator CARPER. Give us some idea what that schedule is. That would be——

Dr. BUDETTI. That is——

Senator CARPER [continuing]. Forty-two plus about 58, so that is about a hundred.

Dr. BUDETTI. All of the ones who are in our Zone Program Integrity Contractors (ZPICs), the anti-fraud contractors who will be using the system. I am told that they are all on schedule to be trained this year, and so that is—we did have to, after getting feedback from the people who were trained in the initial courses, we did redesign the program. We had some user feedback and realized that we were not—the agency was not adequately preparing them for using the system. These are complicated systems and the training program was restructured and revised and we believe it is now an extremely effective one and we have moved forward with an aggressive schedule. We have trained 55 and we are going to finish the ZPIC staff training, I am told, this year. So that is a very important aspect of all of this.

The other thing I would tell you is that the Integrated Data Repository will be one of the sources of data that we will be using in the sandbox that I described, so that the Integrated Data Repository, which holds all of the claims over a prolonged period of time, is very different than the claims processing system that we are using with our new predictive analytics. So one is a repository and one—the IDR is a repository that will hold all the information. The other is being implemented on top of the claims processing system. So they will go hand-in-glove.

We are moving forward. We already have the Medicare claims data in, as you described. We anticipate finishing the different stages of the Medicare data by next year and we are moving very aggressively with a variety of systems to improve the Medicaid data, as well, and doing that in a way that we believe will serve a variety of purposes, both for the States and providing access to the States and also for our purposes, both fraud fighting and otherwise. So I——

Senator CARPER. I am going to ask you to hold there. I am well over my time——

Dr. BUDETTI. OK.

Senator CARPER [continuing]. So I want to be fair to my colleagues. When we come back, I am going to ask our friend from GAO just to respond to what we just heard from Dr. Budetti——

Mr. WILLEMSSEN. Sure.

Senator CARPER [continuing]. And if you can tell us whether or not we should feel reassured. Do not do it now, but I am going to ask you to tell us if we should feel reassured by what he has just presented, all right? Thanks.

Dr. BUDETTI. Thank you, sir.

Senator CARPER. Senator Brown.

Senator BROWN. Thank you, Mr. Chairman.

So just to followup a little bit, so 41 people, and you are training another 55, so you are a little under a hundred. You are supposed to have 639 done by the end of the fiscal year, and I have a little

sheet here to look at. We have 41, so we can increase that a little bit. We are supposed to have 639 and it looks like we are a little short. Ultimately, when we get it done, we have spent $100 million, if I am not mistaken, on this system and we are trying to obviously identify, for example, despite deployment of the One PI program, Medicare fee-for-service (FFS) improper payments amounted to $34.3 billion for Fiscal Year 2010, an astonishingly high rate of 10.4 percent of all Medicare fee-for-service payments. So when will they be all trained? You are saying that the remaining 539, give or take, will be trained by the end of this year?

Dr. BUDETTI. The 55 that have already been trained and the rest of the workers in our contractors will all be trained by the end of this year. We are also doing training for law enforcement personnel and other——

Senator BROWN. Yes, but in terms of the 639, though——

Dr. BUDETTI. Well, the 639 was a number that was established as a goal a number of years ago, and whether that is ultimately the correct number, we are constantly revisiting who needs to use what in terms of fraud fighting capabilities. But we are proceeding with both the law enforcement personnel and with the ones in our contractors on a newly structured training program and an aggressive schedule. So I can tell you exactly how many people we plan to train by when, but I can tell you what I have said so far, which is what we have done to date and what we expect to do the rest of this year——

Senator BROWN. Right.

Dr. BUDETTI [continuing]. So that will——

Senator BROWN. Thank you. You said, though, this was implemented quite a few years ago and——

Dr. BUDETTI. Right.

Senator BROWN [continuing]. We have started the program, and yet quite a few years ago, still have only done, as of recently, under 100 of these folks to implement this system that is a $100 million system. I mean, are we getting a good value? Is it reaching its full potential? It does not seem to be, but maybe I am missing something.

Dr. BUDETTI. Well, I think we—we have admitted that there have been some deadlines that we had established that we did not meet, and we are now working——

Senator BROWN. Well, what ones have you actually met?

Dr. BUDETTI. All of the Part A and Part B and Part D data were put into the Integrated Data Repository in terms of the post-payment data, in fact, as I understand it, I think two of those were actually put in ahead of schedule and the additional data to support the use has also been put in.

I would like to emphasize that the IDR with the One PI system on top of it is a very valuable tool. We are moving to fully implement it. It is not the only resource that is available either to us or to our fraud fighting partners, either in law enforcement or in our systems. But it represents a major step forward. And in terms of the savings, we believe that the savings from moving forward with the IDR will not only be reflected in the fraud fighting capabilities, but also efficiencies in our contracting structure, because

instead of having a series of small data systems set up all around the country, we will have this one integrated system.

So we are moving forward with that, Senator, and we do view it as valuable. But I want to emphasize that it is not our only fraud fighting tool.

Senator BROWN. Sure. I understand that. Do you know if the $150 million or so spent on either system has been a good investment if no outcome performance metrics have been established to measure their actual benefit?

Dr. BUDETTI. So one of the things that we did commit to in concurring with the GAO's report was to establish and put into place a measurement of exactly those——

Senator BROWN. Have you done that?

Dr. BUDETTI. This is what we have now committed to doing.

Senator BROWN. Oh, OK.

Mr. Morris, on the PPACA legislation that provides additional funds to strengthen the program's integrity, it contains other fraud prevention provisions such as the ability of CMS to withhold Medicare payments to providers or suppliers. States also have this ability in the Medicaid program. How many payments have actually been withheld, if you know?

Mr. MORRIS. We took a look at our data and it appears that since the passage of the Affordable Care Act, there have been 53 payment suspensions which were initiated at the Inspector General's request——

Senator BROWN. Fifty-three out of how many? Out of billions, right?

Mr. MORRIS. Oh, of potential payment suspensions?

Senator BROWN. No, out of payments, how many have actually been withheld?

Mr. MORRIS. Well, we identified approximately $8 million in money that was either on the payment floor, about to go out to the target of an investigation, or money that was otherwise stopped. So the 50 payment suspensions I referenced realized a withholding of about $8 million in monies in the Trust Fund. We have been working with CMS to strengthen this process. We have entered into an memorandum of understanding (MOU) that will facilitate more rapid exchange of information, and particularly in our strike force areas where we are identifying career criminals. These are not health care providers.

Senator BROWN. Sure.

Mr. MORRIS. These are people exploiting our program. Payment suspensions are more and more becoming the standard.

Senator BROWN. Great. As the opportunity for fraud grows with the expansion of Medicaid, will CMS be able to meet the added threat, or is it inevitable, as with past expansions of benefits, that it will lead to more fraud, or is it a kind of in between?

Mr. MORRIS. Well, certainly with the expansion of the benefit and thus an increase in the volume of claims, there will be a greater threat to the program. But we think that if many of the provisions that are both in the Affordable Care Act and are part of the program integrity efforts that Dr. Budetti has been talking about are implemented, there should be safeguards.

For example, effectively screening at the enrollment so that we only let in honest providers will go a long way to keeping the crooks out of the system. Similarly, having payment methodologies that reflect what the true cost of a service is and does not have enormous fluff which is then used to perpetuate a fraud scheme, and making sure that we are actually paying for legitimate services. These sorts of internal controls will go a long way to protecting the Medicaid program as it expands.

Senator BROWN. Thank you, Senator Coburn.

Senator COBURN. [Presiding.] Well, I thank each of you for your testimony. I was not a big fan of the Affordable Care Act, but the fraud provisions in it, I readily support.

And I want to emphasize this next point in as nice a way as I can: Having the testimony at 9pm last night for a hearing that has been announced, getting questions for the record (QFRs) answered last night from 3 months ago from a Finance Committee hearing is not acceptable for us to be able to do our job. And my hope would be that those of you that turned in your testimony or your QFRs late would understand that. Otherwise, it seems to me the way we get QFRs answered is have another hearing, so we will have another hearing in 2 weeks to get our QFRs back because that seems to be the only way to get them back.

Dr. Budetti, what is the cost of the new contract with Raytheon? And is it a cost-plus contract?

Dr. BUDETTI. The new contract with Northrop Grumman and their subcontractors——

Senator COBURN. With Northrop Grumman, yes.

Dr. BUDETTI [continuing]. Is set at $77 million for just over a 4-year period. It is an initial implementation period of several months followed by 1 year of award, and then there are 3 years, three option years to follow.

Senator COBURN. So that is a fixed-price contract?

Dr. BUDETTI. That is my understanding, sir, yes.

Senator COBURN. Well, you all have let that contract, correct?

Dr. BUDETTI. We let the contract.

Senator COBURN. OK. So it is a fixed-price contract and——

Dr. BUDETTI. I know that there is a cap on it of the $77 million. That much, I know——

Senator COBURN. And my question is, this is a great company. I do not have any problem with it. When was the last—did they have experience in doing predictive modeling for the insurance industry?

Dr. BUDETTI. So the system that Northrop Grumman and its partners put forward was one that was developed for the private sector, was developed and used in Verizon. They used it for their own transactions and also for their credit card transactions. And part of our solicitation requirement was that the system would be immediately applicable to Medicare claims processing, that there would not have to be a major startup period. And so they partnered with the National Government Service (NGS) and they were able to demonstrate to the satisfaction of the people who were reviewing the proposals that they could apply this immediately, and, in fact, we have been able to show that is actually happening.

Senator COBURN. Good. What is your goal? You have showed us what the plan is with IDR and One PI. What is your goal in terms of fully implementation of predictive modeling on everything that CMS does?

Dr. BUDETTI. As of, actually, June 30, July 1, all Medicare fee-for-service claims nationwide are being screened before the claims are paid. Our goal is to advance that, to build into the system more and more of our analytics. Our goal is also to develop the ways that we can then apply this, as well, to the Medicaid program. That is a very different set of challenges. We are committed to doing it. We are also—we are already beginning to look at that, at the possibilities of doing that.

But we have the system in place and operating nationwide and it is looking at all Medicare claims right away. It will become more sophisticated. It will add more and more analytics, and we also will then be taking great care to make sure that we are interpreting the results properly and going after the bad guys and not the good guys with it.

Senator COBURN. What percentage of claims that are going through this now are halted for review?

Dr. BUDETTI. At the moment, what we have done is put it into place in a way that we have the ability to stop the claims before they are paid, but we want to get a track record. We want to get some traction here in terms of knowing what to do with respect to the kinds of risk scores that we are getting.

We are getting some very impressive results. We are getting some—a very large number of fraud risk scores. But we do not know for sure yet that those are fraudulent. Now, many of the——

Senator COBURN. So you are going on and paying these claims?

Dr. BUDETTI. I am sorry?

Senator COBURN. So they are going on and being paid at this point?

Dr. BUDETTI. We are taking a much closer look and we are exploring the ways that we can take action right now on an administrative basis before they get paid.

Senator COBURN. But right now, of the claims that come through——

Dr. BUDETTI. Right.

Senator COBURN [continuing]. And they get flagged, what percentage of them are the payments halted on and what percentage are gone on and paid?

Dr. BUDETTI. Well, we are 12 days into it and right now, what we are doing is taking the results of the most egregious findings that we have, taking those to our new rapid response system that we are setting up to get our contractors to look more carefully—our Zone Program Integrity Contractors to look more carefully at them. And if it comes back that our strong suspicions are confirmed, we will have the ability to stop those payments. So I am not ready to tell you that we are—we are—yes, we are making payments now, but we are positioning ourselves to be able to stop them. But we want to do this correctly. We did not set this up to automatically stop claims on day one because we wanted to make sure that we were getting results that were responsible first.

Senator COBURN. All right. Then let me get you on the record. When is it that you are going to have suspicious claims stopped pay?

Dr. BUDETTI. I expect that we will have some suspicious claims——

Senator COBURN. No. Every one of them is being reviewed now, every one of them that hits your risk profile. When is it CMS is going to quit paying those claims and send them for review?

Dr. BUDETTI. That is exactly our goal, Senator Coburn.

Senator COBURN. But when?

Dr. BUDETTI. Well, let me—so my answer is that, first of all, we get a risk score that covers a very wide range. So we are taking the very top, the most egregious ones. We are looking at them, first of all, to see whether or not they are already under law enforcement investigation of some kind. We do not want to interfere unnecessarily with a law enforcement investigation if there is one underway. And then the others we are looking at very carefully to start—and we expect to start cutting off payments very soon.

I am not going to give you an exact date because we are going through this process for the first time. We are going through it in a responsive and responsible way. But we are set up for doing this and we will have the system integrated into the—fully integrated and automated into the claims processing system over the course of the next year. But at the moment, we are going to do it ourselves, taking the time to make sure that we are not interrupting claims payments that should not be interrupted.

Senator COBURN. Yes, I agree. So I guess the answer is, within a year——

Dr. BUDETTI. Within a year we will have——

Senator COBURN [continuing]. You plan to have this implemented and working so that we are not sending payments to——

Dr. BUDETTI. We will stop making payments sooner than that, but we will have it fully—we will have it set up so that we are interrupting on a much more rapid basis the claims that fall into the patterns that we have confidence should be interrupted.

Senator COBURN. Yes.

Dr. BUDETTI. And, yes, this is a step-wise process, but we are committed to getting there and we are going to get there. This is the whole purpose of doing it. We want to stop these payments before they go out the door, but we want to do it right.

Senator COBURN. OK. All right. Thank you.

Senator CARPER. [Presiding.] I think you can feel Senator Coburn's sense of urgency, and it is one that we all feel.

Senator McCaskill, good to see you. Welcome. And thank you very much for cosponsoring our legislation.

Senator MCCASKILL. Yes, thank you.

Senator CARPER. We very much appreciate your interest and your leadership.

Senator MCCASKILL. I apologize. Just say if there is any question I am asking that you have been asked before. I could not get here at the beginning of the hearing. I wish I could have, and I want to make sure I do not cover any ground that has already been covered. Did Northrop provide CMS an off-the-shelf product for this?

Dr. BUDETTI. The product that Northrop Grumman and its partners provided to us was built on the one that Verizon and its subsidiary had developed for use within the telecommunications industry, both for their telecommunications fraud and for their own credit card transactions. What the partnership together provided was an approach that was proved in one industry but that was immediately applicable to the Medicare payment system, which, of course, is very different than either telecommunications or credit card transactions. So this is the system that was selected. This is the one that has shown itself to be capable of being implemented immediately and is now up and running on all Medicare fee-for-service claims as of the beginning of this month.

Senator MCCASKILL. I am cynical about buying IT systems because my experience in the Armed Services Committee and, frankly, dealing with other parts of government in contracting issues is that if we say we want somebody to do something, typically, they say they are going to design a system and it takes years and a lot more money than we thought it was originally going to take. Then, ultimately, sometimes it does not even work like it is supposed to and it gets abandoned. And so it is interesting to me that you were able to essentially get an off-the-shelf product. Was it specified that you wanted an off-the-shelf product?

Dr. BUDETTI. We specified that we wanted a product that had been proven in the private sector that could be immediately applicable to the Medicare system and that was capable of being implemented to meet the rather impressive time line that we were working under, and we met all of those requirements.

Senator MCCASKILL. OK. I think it is great that you were able to do that and I wish the rest of government would take note that we are way behind in terms of the integration of data and the systems that are available for analysis in government and we use the excuse of siloed agencies and we want our own system and, well, we have already got this and it needs to talk to that. Way too often, we are not specifying that we want something that has already been proven that, frankly, is off the shelf. That is the good news.

Now, the bad news. IDR was supposed to contain Medicaid data, and we began this, what, in 2006?

Dr. BUDETTI. Yes, Senator. You are correct that there are some, as I mentioned a minute ago, there were some deadlines that the agency had set out, some goals that the agency had set out that, for a variety of reasons, were not met. One of them was the full integration of Medicaid data into the Integrated Data Repository. There are a number of reasons why that did not happen——

Senator MCCASKILL. Give me, like, the top three.

Dr. BUDETTI. The top three are, No. 1, the States really were not under any requirement that they had to submit the data to us. They also faced serious resource constraints. They also have their data in many different formats and many different systems, and so the integration of those into one place was complicated. And as I understand it—this, of course, was all somewhat before my time here—and I also understand that the way that the initial design for the system was structured, that it might have made it more difficult to get the Medicaid data into it.

Those are all things that we are well aware of as the major initiative to get much better Medicaid data, both for the States and also for the Federal Government. That is very much a cross-CMS initiative. It is not just program integrity. It involves the Centers for Medicare and Medicaid Services, the Children's Health Insurance Program (CHIP), and survey and search the MCS, as well, and there is a great deal of work going on to improve that system.

But we do expect to be able to phase in the Medicaid data over time, and in the meantime, we are doing quite a bit working with the States directly, as well.

Senator MCCASKILL. What is the date that you think you will get the Medicaid data in?

Dr. BUDETTI. We are currently targeting 2014 for the ultimate, but that includes the entire revised system that we are talking about that would be restructured and much more useful for everybody. In the meantime, we are working very closely with individual States and with other approaches, and we are currently exploring ways that we can apply our predictive modeling system, which is not exclusively dependent on or the same as the IDR, ways that we can work with the States to use the predictive modeling approach, because we do not get the same flow of claims data directly to the Federal Government for Medicaid that we get for Medicare. Medicare, we get their claims. They send us their claims——

Senator MCCASKILL. Right.

Dr. BUDETTI [continuing]. Because they want to get paid.

Senator MCCASKILL. No, I understand.

Dr. BUDETTI. And in Medicaid, we are dependent upon the States who are processing the claims——

Senator MCCASKILL. And they are dependent on our money.

Dr. BUDETTI [continuing]. To report to us, and they are dependent upon our money and other resources——

Senator MCCASKILL. And I have found that can be a very persuasive tool.

Dr. BUDETTI. And that is a challenge to everybody, yes. Yes, Senator.

Senator MCCASKILL. Yes. And I think the more that you begin to exercise that muscle, I think the more cooperation you will get from the States. They are all gasping right now and incredibly dependent on the help that they are getting from the Federal Government, and I, for one, think that it makes more sense that we are giving them that help as opposed to jacking up costs for everybody by all the uninsured care that would occur the more we cut back on the Medicaid program. So I encourage you to use that muscle, that we have money and you need it to get the data that we need to provide the integrity to the program.

Let me know the acronyms, you all are not nearly as bad as the Department of Defense (DOD), but you have a dizzying array of contractors that are supposed to be fighting fraud. We have the MACs, the Recovery Audit Contractors (RACs), the ZPICs, the Program Safeguard Contractors (PSCs), and that is not counting the IDRs, the IDIQs, and now the new program. Obviously, all these contractors that were supposed to be doing all this, it has not worked out as well as we hoped. What are you doing to clean up this mess in terms of how many contractors we have and is every-

body on the same page, is everybody working together, are we working at cross-purposes? What efforts are being made to allow people to track how well we are doing on integrity without a scorecard?

Dr. BUDETTI. Senator, it took me several months on the job to get all those acronyms down and I do not think I have mastered all of them yet. But in answer to your question, we are doing a number of things. For one thing, we have restructured the way that we are overseeing our anti-fraud contractors, the Zone Program Integrity Contractors, and we are working to finish the transition to have Zone Program Integrity Contractors uniformly across the country.

We have also assigned more staff. We are conducting onsite reviews instead of paper reviews. We have a number of oversight changes that we have put into place. We have put them under a new group within the Center for Program Integrity. We are doing a lot to improve our oversight of those contractors.

The Medicaid administrative contractors, the ones that handle the claims, of course, are responsive to a number of different components within CMS, but we are working very closely with them, as well. They interact with the Recovery Audit Contractors, the RACs, as well.

We have done a lot to improve the ability of the programs to work together. One of my goals is exactly that, to have a much more efficient system. One of the characteristics of our new fraud prevention system that is very useful is that it is also a management tool, because as we do these analytics and we send to the Zone Program Integrity, the anti-fraud contractors, we send them the results and say, here are 10 people with astronomical fraud scores. Do something. Look at these real carefully and get back to us right away. That is our rapid response strategy that we have developed. That is a new use of the interaction with them, but it is also a management tool because we know when we sent them that information and when they responded. So we have a number of——

Senator CARPER. Dr. Budetti——

Dr. BUDETTI [continuing]. Doing this.

Senator CARPER. I am just going to ask that we draw—finish your sentence, but then——

Senator MCCASKILL. No, I do not have any more. I just wanted to—

Senator CARPER. No. Go ahead and finish your sentence and we will have a second round, I promise.

Senator MCCASKILL. Yes. I would just——

Senator CARPER. Go ahead and finish your sentence, Dr. Budetti.

Senator MCCASKILL. The only request I would make for the record is if you could provide me a flow chart of all of the different anti-fraud contractors that are currently working for our Federal Government and how they work together and what their responsibilities are. Somebody someplace has diagramed that out, I bet.

Senator CARPER. Would that be with or without acronyms? [Laughter.]

Senator MCCASKILL. It would be helpful if the acronyms would be front, bold, and center, because I think for oversight purposes,

it is going to be helpful for us to understand how they work together now, and then hopefully when you come back in a year or two and show us the $20 billion a year you have saved, you can point to which part of the system worked and we can get rid of some of these contractors that are not working.

Dr. BUDETTI. I will be delighted to do that for you, Senator.

Senator MCCASKILL. Thank you, Mr. Chairman.

Senator CARPER. I want to lower expectations. It is actually $20 billion over 10 years, but if you can do the $20 billion a year, we will take it.

I said earlier when I was asking the first round of questions and my time was expiring, I said I was going to come back to, I think I said to Mr. Willemssen, but I am going to ask the other witnesses to do this, as well. I want you to reflect on what Dr. Budetti has said in his testimony and his responses to our questions. What should we feel good about? What should we feel concerned about? Do you want to go first, Mr. Willemssen?

Mr. WILLEMSSEN. Certainly, Mr. Chairman. One, we are pleased that CMS has concurred with all seven of our recommendations and planned to act to implement those recommendations. If they act appropriately and implement them fully, then we can see figures like that $21 billion on the chart up there.

Second, I do not want to underestimate the——

Senator CARPER. Now, how do we make sure that they actually follow those recommendations? You give them the recommendations. They say, yes, these are good recommendations——

Mr. WILLEMSSEN. That would be my second point——

Senator CARPER. OK.

Mr. WILLEMSSEN [continuing]. And that is related to committing to milestones and deadlines on when those actions are going to be put in place. For example, when will CMS put in place the ability to establish tracking mechanisms associated with those two systems to demonstrate what kind of benefits are we getting and what kind of cost reductions are we getting, what kind of fraud are we identifying and preventing?

And a third point is related to the Integrated Data Repository. I do not want to underestimate how important that is. That is a tremendous tool, to have one massive database——

Senator CARPER. Let me interrupt here just a minute. If somebody on the other side of the moon were listening in to this conversation and trying to understand what an IDR is, who can explain it so that a regular person off the street or just a mortal like me——

Mr. WILLEMSSEN. One way to think of it——

Senator CARPER [continuing]. Could actually understand it and it actually be meaningful.

Mr. WILLEMSSEN [continuing]. Is if you are——

Senator CARPER. Give me a good example. Somebody just give me a good example of this, OK, and I do not care who does it.

Mr. MORRIS. The way I have been led to think about it, because I do not understand it, either, is that instead of going to five little grocery stores to pick up all the parts you need for a dinner, an IDR is a supermarket where you get all the components, all the information you need to build your dinner.

Senator CARPER. All right. That is great. Even I understand that.

Dr. BUDETTI. And the One PI system that sits on it is the recipe book.

Mr. WILLEMSSEN. Yes. Very good.

Senator CARPER. All right.

Mr. WILLEMSSEN. In fact, it would give you instant access to the data you are looking for because you do not have to go through a lot of iterations. It is sitting right there on your desktop. So I want to emphasize the importance of that, and that is why it reinforces why we get as much data on there as possible.

In terms of concerns, I am a little bit concerned with the change in going from an incremental approach to adding State Medicaid data to now the approach will be to do all 50 States in September 2014. Our experience shows going in an incremental fashion is often a more prudent risk-based approach, kind of a lessons learned, what works, what does not. So just based on what I heard and what I know of, doing all 50 in 1 month in 2014 sounds a little risky as opposed to the incremental approach.

Senator CARPER. Would you suggest that the course we take would be to maybe start with the first State that ratified the Constitution, then the second State? [Laughter.]

Mr. WILLEMSSEN. I will defer to you, Mr. Chairman.

Senator CARPER. All right. OK. Thanks for those responses. Mr. Saccoccio.

Mr. SACCOCCIO. Yes. We are very excited about what CMS is doing, and we understand it is going to take some time. But when you look at the Medicare system, and then if you bring the Medicaid data, as well, there are enormous opportunities there, because unlike on the private side where, say, an Aetna has its own data or Cigna has its own data or Blue Cross-Blue Shield of Louisiana has its own data, here—and although they could take a look at that data, they are looking at a very small slice of what is going on out there.

With Medicare and Medicaid, because of the enormous numbers and integrating all of that data into one place, there is enormous opportunity there not only for Medicare and Medicaid as they begin to analyze that data, suspend payments go after fraud, but then to take that information and share that information also with the private side, as well, not giving the private side access to the data, but taking the trend information that they see, the schemes that they see arising out of that data.

For example, J codes, the codes used for infusion therapy are being abused in South Florida and we are starting to see a lot of that based on the analysis that we are doing. Let the private side know, the payers that are in those areas know that they should look at their data so that they can focus efforts, too. So I think it is an enormous opportunity, given the enormous amount of data that is there for Medicare and Medicaid.

Senator CARPER. All right. Thanks.

Mr. Morris, what should we feel encouraged about and what should we still have some concerns about?

Mr. MORRIS. From the perspective of the Inspector General's Office, we are very pleased with the sense of partnership and CMS's interest in engaging us in designing a system that works for law

enforcement as well as program integrity. And having worked in the IG for a number of decades, I can tell you it is refreshing compared to prior interactions we have had with CMS.

I would say areas of concern, as touched on in my written testimony, we think it is going to be critical to monitor how the contractors perform in this context because our past experience is that contractors oftentimes disappoint us.

The other particular interest we have is moving to what we call real-time data. Much of the information that we use as part of our criminal investigative work is pre-adjudicated. It is data that has not been scrubbed and perhaps may not even get paid. But it tells us that criminals are pinging the system. They are testing to see where claims get rejected because then they shape their strategy around those screens. So knowing when a criminal has tried to get in and has been unsuccessful is as valuable to us for fraud detection as spotting the claims through the predictive analytics. It is what we are building on. It is something we look forward to getting.

Senator CARPER. All right. That is a good point.

Dr. Budetti, just take a minute and respond to what you just heard from your three colleagues here, just a minute.

Dr. BUDETTI. Senator, I think that we are very encouraged by the partnership that we have been able to establish with the Office of Inspector General and our other law enforcement colleagues and I will be delighted to look at whatever suggestions the GAO has for other ways to implement the Medicaid data. I will tell you that there is a lot of work going on right now to try to make sure that we are in position to be able to do that and do it properly.

Senator CARPER. All right. Thanks. Senator Brown.

Senator BROWN. Thank you, Mr. Chairman, and you asked a good question, Mr. Chairman, about IDR and explain it for the average person listening at home. Doctor, you referred to it as a recipe book and then a grocery store. It is interesting. It is a recipe book and a grocery store that does not have all the required items to either look up or purchase. The shared systems are not in there. There are a lot of holes in it.

So I am curious, like, when is the recipe book going to be completed and the grocery store going to have all the products you need, because every hearing that I participate in, it is, like, oh, yes, we all get along. Everyone is great. We agree with this. We agree with that. And at the end of the day, we are kind of in the same situation, and doing the legislative history and the committee histories as we have done, being the newer person here, it is like deja vu. It is like Groundhog Day. You hear the same thing over and over and over. You have a new guy coming in. He has all the greatest intentions and he is picking up the slack where the other person left off and here we are.

So I guess my question ultimately is to you, Mr. Willemssen. You have testified previously that one system, the old Medicare Transaction System (MTS), was terminated after we spent $80 million, and you stated that it was a huge learning experience. Yes, it was a very expensive learning experience, too, in my estimation. In your opinion, at this point, has CMS learned from its past failure

and do you have confidence that they will be able to meet its stated deadline of 2014 for incorporating all Medicaid data into the IDR?

Mr. WILLEMSSEN. Yes——

Senator BROWN. That is the recipe and grocery store we were just referring to.

Mr. WILLEMSSEN. I did testify on that failed Medicare Transaction System about 14 years ago. There are similarities. There are differences. One of the similarities and lessons learned is there was some underestimation of complexity going into this.

One area I would point to is in Medicaid. When asked earlier, Dr. Budetti talked about three reasons that made it difficult for why those were problematic in bringing into the IDR. I would echo the third reason that he talked about. All those State Medicaid Management Information Systems are separate. They often have different data element definitions and different file structures. So trying to aggregate those all together is very difficult.

So we are encouraged to hear that there are efforts underway to do that, but I think the way you have to hold the agency's feet to the fire is you have to have them commit to milestones and deadlines——

Senator BROWN. Right, and——

Mr. WILLEMSSEN [continuing]. On when are certain activities going to be done, and we would like you to come and—the way to enforce that, continuing congressional oversight. I think there were comments earlier about QFRs coming at a certain point in time relative to a certain hearing. There is a lot to be said for congressional oversight and actions that get taken.

Senator BROWN. And it is interesting you say that, because my next followup question was, what are key indicators we should look for to ensure that these progress results are being made.

Mr. WILLEMSSEN. The key indicator I would look for is to ask CMS what kind of benefits are accruing. Now that they have agreed to implement a system to track those benefits, what is happening? What kind of fraud reduction are we accruing? What kind of chunk out of that $21 billion, which, as the Chairman mentioned, was for a 10-year period, but that 10-year period was 2006 to 2015, and right now, CMS does not know if they have accrued any benefits.

Senator BROWN. Right. That is part of the problem that the Chairman and Senator Coburn and others have been working on before I got here. But, I guess, getting back to you, Dr. Budetti, how can you convince us that this time—and when I say "you," it is not you, obviously, because you are new—your entity, your group that you are representing, how do we know that you are going to get it right this time? What confidence should we have?

I think we are kind of optimistic here. We will try to work together. The Senator and I, out of the people that work here, are probably the two closest people that work together when we have an opportunity. What assurances can you give us that, in fact, you are getting it right this time, based on previous testimony and previous experiences?

Dr. BUDETTI. I appreciate that question, Senator Brown, and there is a lot of history in a lot of these situations that it is important for us to learn from. All I would cite is one example, the fact

that we did get a major system implemented and up and running within 9 months of when the President signed the legislation and it has already reviewed all Medicare claims for the last 12 days and that we are setting up systems to deal with the results of that.

Senator BROWN. And if I could just interrupt——

Dr. BUDETTI. Certainly.

Senator BROWN [continuing]. I want to congratulate you on that. Aside from just throwing bombs, I think it is important to recognize a good job, as well, so congratulations on that effort.

Dr. BUDETTI. I appreciate that very much, and, of course, I pass along your nice words to the people who actually did the work, who were my colleagues.

The other thing I can say is that I think that you have heard from me before and you know that the intense commitment that we bring to this task. I think this is something that we want to accomplish, we are dedicated to accomplishing. We want to know exactly the kinds of results that the GAO mentioned, which is we want to know whether this is working, and we are developing metrics. We are looking to be able to measure not just money that we recover, which is very difficult in some of these situations, but in avoidance of payments that otherwise would have gone out the door. So we are, in fact, developing those metrics and looking at the ways that we can collect those data and I am delighted to continue with your oversight and report back to you regularly on our progress.

Senator BROWN. Thank you.

Mr. Saccoccio, you look lonely, so I wanted to ask you a question. [Laughter.]

In your testimony, you discussed how FICO, an expert in credit risk analysis, was built on its expertise in the financial services industry to provide a predictive modeling for the private health care industry. Are any of your members currently using predictive modeling to prevent fraudulent payments?

Mr. SACCOCCIO. Yes, several are. On the private side, it is kind of a mixed bag in the sense that you do have some companies that are well ahead of others. Obviously, you have the national companies that have more resources than, say, the smaller regional insurers. But some of them are using predictive modeling. They are trying to get a handle on the whole prepayment thing. Remember, it is not just an issue of predictive modeling but when are you applying it. Are you looking at claims before they are being paid or are you taking a look at them after they have been paid.

So the push is to try to do this prepayment as much as possible, and that is a real challenge because there are requirements to pay claims in a certain amount of time. Every State has a prompt pay law. ERISA requires claims to be paid in a certain amount of time. So the private payers do have that pressure to try to pay those claims as quickly as possible, which then kind of offsets some of their efforts on the prepayment side.

But some of the companies have started to use predictive modeling. Some are ahead of others. They all have some sort of data analytics that they do, but they are all moving in that direction with the emphasis trying to be pushed to the prepayment side of things.

Senator BROWN. All right. Thank you, Mr. Chairman.

Senator CARPER. No, thank you.

One of the things that Senator Coburn and I had worked on for a number of years was the issue of improper payments, and the earlier legislation, I think, passed in the first term of George W. Bush on improper payments, I think basically said, Federal agencies, we want you to be mindful of improper payments and start writing them down, or at least noting what they are.

Senator Coburn and I came back a year or so ago and legislation signed by President Obama basically said, we not only want you to note the improper payments, we want you to stop making them. Federal agencies, we want you to report them. And last, we want you to go out and recover as much money as you can from those improper payments, particularly when there are overpayments that were made. And we had a fair amount of discussion in this hearing room in the past on recovery audit contractors, folks that literally we send out to recover overpayments, in some cases fraud, in other cases just mistakes.

One of the questions that we got into here—I think, Dr. Budetti, we discussed this with you and the folks at CMS in the past—but just give us—I think maybe when you appeared at our last Subcommittee hearing on this topic, I think you said that CMS plans as expeditiously as possible to implement the final rule on Medicaid recovery audit contracting, and I think that was in the early part of maybe March this year. It has been 3 or 4 months. And now that we are meeting again in July, could you give us just maybe a more definitive date on when the final rule for Medicaid recovery audit contracting might be issued.

Dr. BUDETTI. Thank you, Senator. Yes, I did use words probably to that effect. I have also said that it would be forthcoming soon. We do expect——

Senator CARPER. Those are the kind of answers that we give. You are not supposed to do that. You have to be more specific.

Dr. BUDETTI. I can never commit to a specific date on a——

Senator CARPER. I have noticed that.

Dr. BUDETTI [continuing]. Promulgating regulation.

Senator CARPER. That troubles me.

Dr. BUDETTI. But we are expecting this to be out by the end of the summer.

Senator CARPER. The end of the summer, OK. Now, could that be, like, September 21?

Dr. BUDETTI. You are very good at knowing the calendar, Senator. [Laughter.]

Senator CARPER. Well, sometimes, like on the beaches, we close our beaches down on Labor Day, so we will see. OK. End of the summer. We will take your word on that.

I want to go back to the—this is really one for all the panelists, and we will start with you, Mr. Saccoccio, and this is regarding public-private partnerships. Sometimes we think fraud is something that only happens in the Federal Government or State Governments or local governments. Actually, a lot of fraud occurs, at least with respect to health care, I am told, with the private health insurance companies.

I once remember talking to folks from MBNA, a big credit card bank headquartered in Delaware, now part of Bank of America.

But I could not understand why they kept hiring all these folks who had been, like, top senior-level FBI and any number of other law enforcement agencies around the country, and I thought, what do they know about credit cards? And as it turns out, they knew a lot about ferreting out fraud and trying to stop it where it raised its head.

A lot of folks in financial services know some things that we could learn from, and certainly the folks in the private health insurance companies that we could then learn from them, as well. And I think, if I understood your response to Senator McCaskill, Dr. Budetti, one of the reasons why we are able to get something off the shelf is because other sectors of our country, our economy, our health care delivery system, they had already worked on this issue and had come up with a way we were able to actually take that off the shelf. I think that is what I heard you say.

But let me just—here is a question to all of our panelists on public-private partnerships. We have heard, I think from each of our witnesses here today, the importance of information sharing, public and private partnerships. Health care fraud criminals target everyone, whether they happen to be a private health insurance company or Medicare, and unless we find a way to work together to identify those who would steal from us, prevent improper payments, and prosecute those who have already committed fraud, we will continue to struggle to root out and defeat these fraudsters. I think it was Mr. Morris—I think it was you, sir—who referred to the public-private partnership, and Mr. Saccoccio has shared with us how the National Health Care Anti-Fraud Association brings together representatives from private insurers and public health care providers.

What I want to ask each of you to do, just take a minute or so, a minute or maybe two, to tell us how those of us in Congress could help strengthen and formalize these types of working relationships or other improvements that we should encourage in these important public-private partnerships. Maybe there is nothing we can do. Maybe there is plenty of incentive just to do it on its own. But if there is something that we ought to be doing, we would like to know about it. Mr. Saccoccio, do you want to go first?

Mr. SACCOCCIO. Sure. Thank you, Senator. I think a lot of, as you discussed, private-public partnerships, a lot of it is something that can be done independent necessarily of additional laws or statutes. But there are some areas that you may want to take a look at.

First of all, with respect to—as we go down the road here with respect to predictive modeling in the Medicare program, is there an opportunity to allow the private insurers, again, access to information, not, again, access to the data, but access to trending information, schemes, those kinds of things. I suspect that a lot of that could be done by CMS without legislation, but to the extent that those issues are addressed in legislation, for example, your FAST Act bill that you have proposed, allowing the private side to participate as much as possible in those types of activities that make sense, and information sharing, obviously, is the biggest one.

The other thing is, are there any other areas of the law that in some way undermine the ability of law enforcement to share information with the private side unnecessarily. Obviously, if there is

a law enforcement investigation, you do not want to compromise that investigation in any way. But if there are some statutes out there that in some ways undercut or undermine the ability to share information that do not make any sense, to maybe take a look at those and maybe look at maybe changing that.

Senator CARPER. All right. Good. Thanks. Mr. Willemssen.

Mr. WILLEMSSEN. I would echo a lot of those comments. I think to the extent—looking at the predictive modeling, to the extent that you can see some best practices and share those best practices, I think you will find a lot of private sector organizations willing to share their tools, in some cases at not that high of a cost because they want to get the word out. They want to be shown as best in class and what they are doing may be at a discounted rate for the Federal Government in a variety of important areas.

I also would second the comment about enhanced information sharing and just to ensure that as that occurs, that we take into account privacy and security considerations.

Senator CARPER. All right. Thanks. Mr. Morris.

Mr. MORRIS. I would first note, as was set out in my written testimony, that since 1996, the law has charged us, the Attorney General's Office and the Secretary through the Inspector General, with working with the private sector to identify ways to share information, and one of the results of that has been the Health Care Fraud Working Groups, which are based in U.S. Attorneys' Offices, many of which have a collaborative relationship with the private side. So encouraging the spirit of the law be embraced and that we look for more opportunities to collaborate would be part of it.

I should also tell you that the Inspector General's Office, through the leadership of Inspector General Levinson, has really pushed for greater collaboration, and one of the things that we have done is undertaken a survey of both our agents, our partners at the Department of Justice, and the private sector to get an idea of what are best practices. What are the work groups doing that are bringing about successful identification and prosecution of fraud, both on the private and public side. We are going to be generating a report as a result of that work and hope to spread the good news about what works and what best practices should be embraced.

The other thing I would note is that bringing people together to share ideas is a great way to identify barriers and break them down, and through the leadership of the Attorney General and the Secretary, we have had a series of HEAT summits around the country where the private sector and government agencies have come together and shared ideas about identifying, preventing, and prosecuting fraud. So I think knowing that the law is in place and then having the commitment of leaders to see that its spirit is met goes a long way to getting greater collaboration.

Senator CARPER. Good. Thank you. Dr. Budetti.

Dr. BUDETTI. I would echo the comments of my co-panelists today, and I would also—the only thing I would add to that is that working together with the private sector is both something that we have done with this particular initiative that we are talking about today, the predictive modeling, but also there is a very strong interest at the highest levels of the Department of Health and Human Services to work out a specific framework for additional inter-

actions with the private sector and working with our colleagues in law enforcement, as well.

So one of the first things we are going to be doing is sharing information on payment suspensions with our private sector insurance companies that provide Medigap plans. If we are not going to pay a claim, why should the Medigap plan pay a claim? But we are exploring many other ways for us to proceed along the public-private partnership to fight fraud. We recognize that everybody has to be in this together, so——

Senator CARPER. Well, might that work the other way for the private health insurance companies if they decide not to pay a claim under the Medigap——

Dr. BUDETTI. Those are the kinds of things that are very much of interest and under discussion, yes.

Senator CARPER. Good. All right. One hand washes the other. Senator Brown.

Senator BROWN. Mr. Chairman, I just have two quick questions, and I appreciate you holding this hearing again.

So when I am back home talking to people about the overpayment issue, I say, you buy an insurance policy. You pay the monthly premiums. You have a beneficiary. That person dies. The beneficiary gets the check, right. Well, in the government's instance, sometimes they get that check three or four or five times, and as a result we have overpayments, or we are paying people that are actually dead and they are not supposed to be getting payments from the government.

So I am wondering, I know in the FAST Act that Senators Carper and Coburn pushed, that requires a daily view of the Social Security Administration (SSA) death master to prevent that type of fraud. Is that something that you folks are doing or plan to do, or would support, or what is that so that we do not keep paying people who are already dead, giving them benefits?

Dr. BUDETTI. Senator, one of the things that we are doing—I have not talked about this today yet, but one of the other major initiatives that we are undertaking, and, in fact, we are in the process of looking for contractors to work on this with us, is to automate the screening process that puts into place the more detailed screening that was required under the Affordable Care Act. A lot of that is being done right now, but it is being done in more cumbersome ways and we are going to be doing it in a way that will be checking databases and will be checking databases as often as is necessary to keep them updated. We are going to be checking on databases continually, not just when people apply to the program, but while they are in the program, on an ongoing basis.

So, yes, we are very much interested. We do not want to pay any claims to or on behalf of someone who was not alive when the service is either delivered or received, and so we are committed to all of the ways that we can do that, and one of the ways is through greatly improving and enhancing our screening process so that we are checking all of those databases and checking them regularly.

Senator BROWN. It would just be nice to have an alert on the screen, "Alert, alert, he is dead. Do not pay him." Something pretty simple.

Dr. BUDETTI. We want to head in that direction, but as you know, when somebody is entered into the death file, they are entered as a person who dies——

Senator BROWN. Sure.

Dr. BUDETTI [continuing]. Not necessarily as a physician, and so we have some other connections to make.

Senator BROWN. Well, governmentwide, I mean, we had a hearing, $150 billion a year that we are giving out in just overpayments. That is a lot of money when we are looking for ways to kind of balance the budget and get our fiscal and financial house in order again.

Mr. Morris, I just have one final question. How concerned are you about cybersecurity, the safety and security of the networks and having people get into private issues with not the best of intentions?

Mr. MORRIS. It is a great concern of ours and we have been doing a lot of work, both with the Office of the National Coordinator, focusing on how to build safe systems as we move into an electronic health record. There is additional work we are doing right now which we would be pleased to brief you about, probably more appropriate in a private setting.

Senator BROWN. Sure. Are you confident at this point that our systems are safe and secure?

Mr. MORRIS. I think there are opportunities for improvement.

Senator BROWN. OK.

Senator CARPER. What I always say here, and Scott has heard this a million times already, everything I do, I know I can do better. That is true for all of us, and it is true here, too. We just have to constantly improve, because the bad guys, they are not stupid and they are testing us and we just have to be smarter, get smarter faster.

Anything else?

Senator BROWN. I am all set, Mr. Chairman. Thanks for holding this hearing.

Senator CARPER. Thanks very much for being a part of it and for joining us in cosponsoring the legislation.

I am going to ask just maybe one or two more and then we will wrap it up.

This would be for, I think, Mr. Morris and Dr. Budetti. Let me just ask a question about the program integrity provisions of the Affordable Care Act, the health care law. There were several provisions of the law, as you may recall, that strengthen new Medicare and Medicaid provider screening. It allowed for the suspension of payments—we have had some discussion of that here today—where there is credible evidence of fraud, and that expanded recovery audit contracting. Since the passage of the Affordable Care Act, the Centers for Medicare and Medicaid Services has taken many steps to implement these provisions.

I would ask, Mr. Morris, maybe you, Dr. Budetti, if you would, could each of you just outline briefly for us the areas where you think CMS has done a very good job implementing a provision and where have we seen the most success. Could you tell us also a little bit about activities that might still be wanting, where CMS should focus more or perhaps where we need improvements to get the

most out of its new authorities. We had some discussion of this already here today. I just wanted you to drill down on it one more time.

Mr. MORRIS. I would say that, across the board, the Inspector General's Office has been very impressed by how quickly CMS has developed the regulations and put into practice many of the statutory requirements. It is no small undertaking and they have really put their shoulder to the wheel. We have seen this in a wide range of the program integrity functions.

If there is one area that we have identified where we think there are opportunities for improvement, it would be in the area of enrollment screening. There are regulations out now that implement the Affordable Care Act's authority to create different tiers of prescreening based on the risk presented by a class of suppliers. We think that there are opportunities for greater flexibility in using those tools and there are ways that we could encourage CMS to use that tool to keep the bad guys out more effectively. But across the board, we have been very impressed by how hard CMS has worked to get these integrity tools in place, and as I have said previously, how open they have been to collaborating with us and taking advantage of our expertise as they have gone through that process.

Senator CARPER. The second half of that question—anything you want to add about activities where CMS's performance might be wanting in this regard?

Mr. MORRIS. Well, I think I touched on one, which is we think there are opportunities to enhance the enrollment screening process. I should say that because so many of these provisions have just recently been implemented, we still need some time to be able to see how they are actually put into effect and some opportunity to study. We will be, as part of our general oversight function, going back and reviewing many of these. Some of them are required by the statute for us to do an assessment, for example, screening of background for long-term care providers. Others, we will be taking on as part of our general work planning. So we will look forward to being able to come up here and give reports of progress as the implementation goes forward.

Senator CARPER. All right. Somebody said to me, I think in anticipation of this hearing today, he said, this is about as exciting as watching wet paint dry. [Laughter.]

For somebody who has—those of us who have worked on these issues for a while, it is actually more exciting than that. What would be exciting is when it gets to be 2024 and we run out of money in the Medicare Trust Fund. What would be exciting is to say to the people who depend on Medicare in 2024 or 2025 or beyond, I am sorry, we do not have any more money to pay for your coverage.

What would be exciting is as we try to get into these deficit reduction negotiations and we can actually say to the President and bipartisan leadership of the Congress we think we can save some money in Medicare and Medicaid that we had anticipated because of the good work that is being done, in part in response to the passage of the Affordable Care Act and in part maybe out of some of the ideas that come out of Senator Coburn's legislation and mine,

ideas that, I might add, were fed to us by some of our friends here at the table from the IG's office and from GAO and from CMS, as well, and from smart guys like Mr. Saccoccio. That would be exciting.

What I want to do is make sure that we have some of the latter kind of excitement and none of the excitement that I talked about earlier, when we run out of money and have to turn to a whole couple of generations of people and say, that great Medicare program that has been around since 1965 is going away. We do not want to do that.

I appreciate the spirit with which CMS has tackled these challenges. Dr. Budetti, how long have you been in your job now?

Dr. BUDETTI. Since February of last year, Senator.

Senator CARPER. I remember the first time we met. Your hair was all dark. It was black.

Dr. BUDETTI. It was. [Laughter.]

Senator CARPER. And here we are, not very much later. But, obviously, you and your folks are putting a lot of effort into this.

One of the things I liked to do as Governor—I still like to do it—is I like to do customer calls. I still call on businesses in our State, outside of our State that have operations in our State, and the questions we ask those businesses are, how are we doing, in this case, the Federal Government or State Government, and what can we do to help you?

And one of the ways I want to close out here is to sort of say, what else can we do on our side, on the legislative side, to help make sure that there will be Medicare around after 2014, and to make sure that some of the savings that we are talking about here actually are available to put on the table to help move these deficit discussions. What else can we be doing? Dr. Budetti.

Dr. BUDETTI. Well, Senator, I just want to express our appreciation for the support and interest that you have shown in this area because that is probably the key for us. We have absolutely terrific tools, both in previous laws but also powerful new tools in the Affordable Care Act and we need to make sure that we continue to have those supported in a way that will allow us to carry out our job. So we look forward to continuing to have your support, and, of course, we are always open to engaging in dialog with you at any time on ways to move even further forward. And I know, as you always say, we are doing a good job, somebody, but they could always do better. Well, we are happy to keep talking to you about that. Thank you.

Senator CARPER. Yes, thanks. Mr. Morris.

Mr. MORRIS. We have had the pleasure of working with your committee staff on a number of ideas around the FAST Act——

Senator CARPER. Are any of them sitting behind me today?

Mr. MORRIS. They are, sir.

Senator CARPER. Do you want to mention any names? Who has been especially helpful?

Mr. MORRIS. I would say Peter Tyler has been amazing.

Senator CARPER. Oh, really. You did not have to say that. How about on the Republican side? We have some pretty good people over here, too.

Mr. MORRIS. So outstanding that I would not even know where to begin.

Senator CARPER. OK, fair enough. [Laughter.]

All right. Well, Peter has mentioned a couple of them to me and we are grateful for the sense of partnership that we have here.

Mr. MORRIS. I could offer as just one example of a small way that we could expand the ability to protect the integrity of the program, under the FAST Act, the bill would expand access to CMS for the National Director of New Hires so they could use that information for their integrity work. We would suggest that you consider also expanding that access to the Inspector General's Office. We would like to use that tool to screen health care providers to ensure they have not hired excluded individuals who might be compromising both beneficiaries as well as the integrity of the program.

Senator CARPER. All right. That is a good point. Thank you. Mr. Willemssen.

Mr. WILLEMSSEN. I would again echo one thing I mentioned earlier. I think continued congressional oversight through hearings such as this can, among other things, help spur action. They can help identify issues. They can identify obstacles that maybe the Congress can assist the agency, in this case CMS, in overcoming.

Senator CARPER. All right. That is good. I am a big believer in oversight. Good. Mr. Saccoccio.

Mr. SACCOCCIO. Senator, I think a lot of the—all the aspects in the FAST Act are very good, especially those dealing with drug diversion. That is a major, major issue now with respect to fraud.

Senator CARPER. Have you heard a price tag put on that?

Mr. SACCOCCIO. No, I would not have a price tag for that, but it is a major problem, and it is obviously not just a financial issue. It is a real person issue, as well, as far as——

Senator CARPER. Yes. Well, take just a second and just explain to the folks that are listening here or following the hearing, the Drug Diversion Act, just tell them what we are talking about here——

Mr. SACCOCCIO. What we are talking about there is basically narcotic-type prescription drugs that are being abused and——

Senator CARPER. Controlled substances, that kind of thing——

Mr. SACCOCCIO [continuing]. Controlled substances, the types that are used many times for pain management, and what is happening is either through providers that are doing, turning their practices into pill mills or patients that go from doctor to doctor to doctor shop to try to get those pills, or pharmacies or pharmacists that may be involved, and basically getting those drugs and then selling them on the street because they have a very high street value and it has just become a very big problem.

Last year, our organization gave our Investigation of the Year Award to a case out of Kansas where, basically, a physician and his wife were running a pill mill that was responsible for——

Senator CARPER. And when you say "pill mill," I know what it means, but why do you not tell others.

Mr. SACCOCCIO. Basically, they were open 24 hours a day and anybody that wanted those narcotic controlled substances could come get a prescription for them without any examinations or anything like that. Basically, you just pay me the money, I will give

you the prescription so you could go out and get those drugs for your use or to sell them on the street.

And based on that investigation that was both a private-public type of investigation, there were at least about 64 deaths that were attributed to overdoses based on drugs coming out of that particular physician's office.

Senator CARPER. That one place.

Mr. SACCOCCIO. That one place. So it is an enormous problem and the State entities that would take a look at drug diversion and try to share that information, some of the provisions that are in the FAST Act, I think, are very important.

But I think the one message that is critically important is that this has to be an effort that is not just focused on 1 year or 2 years. It is going to take a long time. It has to be consistent, and it has to be a continuous-type effort from year to year. I know there is a lot of focus on it right now because of the deficit and trying to find recovery of funds, but it is something that has to be focused on year in and year out and it has to have a commitment by this Administration and, quite frankly, any subsequent Administrations, to just keep at it year after year, and that is the only way that you are going to really make an enormous dent in the problem.

Senator CARPER. Thanks for that. I really think all the testimony has been helpful. The thing that you have done is to remind us that there are human consequences here. It is not just fraud. It is not just money that is being stolen out of the Medicare Trust Fund, but there are real implications for people, for human lives, and I thank you for humanizing this.

Does anybody have anything else you want to add or take away?

I think one of the people I asked, Peter Tyler, I said, who on the Republican side working for Senator Coburn has been especially helpful, and he said, "Well, not Josh Trent—" [Laughter.]

No, he said Josh was a lot of help, so, Josh, thank you, and everybody else who has been a part of that, we thank you, as well.

Well, this is a little bit like a marathon, not a sprint, but like a marathon, and we all just need to stay on task. My hope is if we do that, we will actually save a lot of money and we will help preserve the integrity of this program and we will help restore some fiscal sanity in this country, and to Mr. Saccoccio's point, maybe save some human lives at the same time. So that would be a good day's work.

I thank you all for joining us, for your preparation. What we will do is, I think—Peter, help me, but I think my colleagues have 2 weeks to submit questions and then if they do, I would just ask that you respond to those questions promptly.

With that, this hearing is adjourned. Thank you all very much.

[Whereupon, at 4:25 p.m., the Subcommittee was adjourned.]

APPENDIX

July 12, 2011 Senator Carper

Hearing Statement: "Harnessing Technology and Innovation to Cut Waste and Curb Fraud in Federal Health Programs"

"Today's hearing will focus on two of our nation's health care programs, Medicare and Medicaid, and new steps to help cut waste and fraud in those programs. This Subcommittee has held several hearings about fraud, waste and abuse in these critical health care programs, and we will continue to hold these hearings because, as we do for other programs across government, we must continue to ask this question: 'Is it possible to get better results for less money in Medicare and Medicaid?'

"Today, our nation faces major questions regarding our economy and federal spending. As all of us in this room certainly know, our nation is embroiled in a fierce debate about how to address the country's debt, which totals more than $14 trillion. That debate has now reached a crisis point over raising the federal debt limit, with a deadline of August 2nd.

"A wide variety of ideas have been put forward on how to reduce our budget deficit and begin whittling down our debt. Last fall, the bipartisan National Commission on Fiscal Responsibility and Reform, appointed by President Obama, provided us with a roadmap for reducing the deficit over the next decade by some $4 trillion. This proposal included substantial savings from reducing waste and fraud in our federal health care programs. Achieving these savings will, in many cases, require action by Congress, as well as ongoing effort by program administrators.

"In today's hearing, our Subcommittee will examine some next steps that should be taken to save billions of dollars in waste and fraud in Medicare and Medicaid, which together provide health care for our nation's most vulnerable: seniors, people with disabilities, and low-income children, among others.

"Last year, Medicare paid out about $523 billion to care for 47.5 million beneficiaries. Medicaid expenditures for the federal government and the states were an additional $403 billion. And these numbers are, of course, expected to grow as our population becomes older.

"Americans' increasing reliance over time on Medicare and Medicaid is, unfortunately, translating into increasing levels of waste and fraud. Medicare made an estimated $47.5 billion in improper payments in fiscal year 2010. And this does not even include an estimate for the Medicare prescription drug program, which I'm told could add more than $5 billion to that total. For Medicaid, the improper payments figure is $22.5 billion.

"That's a lot of money. And Medicare and Medicaid continue to be on the Government Accountability Office's list of government programs at 'high risk' for waste, fraud and abuse – as they have been for many years. Now, more than ever, it's urgent that we step up our efforts to eliminate the problems that lead to waste and fraud in these programs. Success in doing so will help us achieve our deficit reduction goals. It will also lengthen the life of the Medicare trust fund, now forecast to run out of money in 2024. Congress has also put Medicare waste and fraud in its sights.

"The Affordable Care Act, which was enacted almost a year ago, includes a number of provisions aimed at enhancing our efforts to fight waste, fraud and abuse in Medicare and Medicaid. Central to the new law is a goal to obtain better results in health care for less money. Eliminating avoidable mistakes and cracking down on criminals will be important elements of achieving that goal.

"Today's hearing will look at some of the innovative steps that the Centers for Medicare and Medicaid Services is taking to reduce improper payments. The Government Accountability Office (GAO) will testify about a new technology-based tool for detecting fraud that could potentially save $21 billion over 10 years, once it is fully deployed. However, as this Subcommittee will learn, while the federal government has made some progress utilizing this effective new tool, it is failing to realize its full cost saving potential.

"To achieve the maximum taxpayer savings, the federal government needs to do a better job of getting this new technology into the hands of oversight staff working to curb the tens of billions of taxpayer dollars lost to waste and fraud in those programs. I will ask our witnesses what more we can do to fully deploy all the tools available to get the job done in our fight against waste and fraud in Medicare and Medicaid and throughout the federal government.

"We will also hear from the head of Medicare and Medicaid program integrity, the anti-waste and fraud office, regarding a recent announcement about 'predictive analytics.' This is technology aimed at preventing waste and fraud by screening claims before payment. This technology is similar to what credit card companies use to analyze customers' spending trends in order to quickly detect and stop fraudulent purchases.

"Furthermore, our Subcommittee will look at additional steps that the federal government should take. Senator Coburn and I, along with several of our Senate colleagues, introduced legislation last month that focuses on fighting fraud, waste and abuse in the Medicare and Medicaid programs, known as the Medicare and Medicaid Fighting Fraud and Abuse to Save Taxpayers Dollars Act, or the FAST Act. The bill includes a wide-range of initiatives and takes some of what we already know works in the private sector to decrease waste and fraud– or that we have already seen is beginning to work in government – and applies it to Medicare and Medicaid.

"Among other things, the legislation would increase anti-fraud coordination between the federal and state governments, increase criminal penalties for fraud, encourage seniors to

report possible fraud and abuse in Medicare through the Senior Medicare Patrol, and would deploy cutting-edge data analysis technologies.

"I often say that there is no silver bullet to fighting waste and fraud. But this bipartisan bill provides many smaller, proven, common-sense solutions that would decrease fraud, waste and abuse in Medicare and Medicaid. It builds on recommendations by the Office of the Inspector General, the GAO and other experts to improve upon the current work of the program integrity office of the Centers for Medicare and Medicaid Services (CMS).

"The FAST Act has garnered numerous letters of support from organizations including the Council for Citizens against Government Waste, Taxpayers for Common Sense, the National Taxpayers Union and AARP, a broad range of groups that don't always see eye-to-eye when it comes to reforming entitlement programs.

"Is CMS moving in the right direction? Yes. But we know what works. We need to do more of it. I believe our legislation takes the same approaches we will hear about today, and does even more.

"Our Subcommittee is here today in large part because, I believe, and I am sure my colleagues believe, that we have a moral imperative to ensure that our Medicare and Medicaid beneficiaries continue to have access to quality care and, at the same time, that the scarce resources we put into those programs are well spent. It is the right thing to do as well, both for the health of those two programs and for our federal budget as a whole. Each and every one of us can agree on that point and, I hope, on a great deal more. I look forward to hearing our witnesses share with us their knowledge and expertise in preventing health care fraud, and learning what more we can do to get better results for less money."

Opening Statement by Senator Scott P. Brown

July 12th, 2011

Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security

U.S. Senate Homeland Security & Governmental Affairs Committee

"Can New Technology and Private Sector Business Practices Cut Waste and Fraud in Medicare and Medicaid?"

Congress is beginning to face the difficult decisions that must be made to put our nation on a path to economic prosperity and fiscal sustainability. One step we can all agree on is eliminating the waste, fraud and abuse which is endemic to the Medicare and Medicaid programs. The waste, fraud and abuse in these programs is estimated at approximately $100 billion a year. That is why I joined Chairman Carper, and Senator Coburn in supporting the "FAST" Act of 2011, which provides a crucial tool to the government for attacking this monumental waste of taxpayer dollars.

Today's hearing is the second hearing in five months that this subcommittee has held. Finding ways to root out waste and abuse in the system is the key to ensuring future viability for these important programs. Simply put, it is no longer acceptable for "business as usual" approach and the endless promises for action while the problem of waste, fraud and abuse continues to grow. This legislation is important and is long overdue.

As I stated at the Subcommittee's March 9th hearing, The Patient Protection and Affordable Care Act expands Medicaid coverage by an estimated 16 million people by 2019 -- a 32 percent increase over the current enrollment in the program. The cost of

Medicaid expansion is estimated to exceed $430 billion over the next 10 years. The federal government is responsible for paying over 90 percent of these increased costs.

This expansion in the government's role in healthcare will unduly strain our nation's already dire fiscal condition and entice predators to gorge on the cash cow which these programs represent. The government's chronic mismanagement of Medicare and Medicaid fraud prevention has landed both programs on the GAO's "high risk list" for many years. Expanding benefits without first establishing the necessary controls to prevent waste, fraud and abuse is putting the cart before the horse. The government's performance overseeing these programs in the last few decades does not indicate a history of success. In light of the burgeoning wave of healthcare spending and the history of lax oversight of these programs, more needs to be done, and done quickly.

Today we will hear about CMS's progress in confronting waste, fraud and abuse through efforts like the creation of an Integrated Data Repository (IDR). The IDR was created to provide a single source of data related to Medicaid and Medicare claims. The IDR began incorporating Medicare data in 2006 but has yet to incorporate any Medicaid data. At the behest of Congress, CMS recently began the use of predictive modeling software to prevent payment of possibly fraudulent claims.

Preventing the payment of fraudulent claims has historically been at the heart of the fraud problem bleeding these programs of badly needed funds as the Government has been forced to pay and chase after the money. While this adoption of technology, long utilized in the private sector such as the credit card industry is welcome, CMS has lacked a sense of urgency in developing and implementing new tools to prevent fraud.

Though Congress has an oversight duty to ensure programs implemented by CMS are effective, CMS should be proactive in pursuing ways to curb waste fraud and abuse in Medicare and Medicaid. Unfortunately, CMS's actions aimed at preventing fraud in recent years have been anemic, at best. It's time that CMS work to fully develop effective programs to eliminate waste, fraud and abuse in Medicare and Medicaid and implement those programs in a timely manner, rather than waiting for Congress to tell them to do something they should have been doing long ago. The American taxpayers expect more from the agency charged with ensuring their hard earned dollars are not wasted through fraud and abuse.

I thank the witnesses for being here today and look forward to a productive discussion on how the government can do better.

STATEMENT OF

PETER BUDETTI, M.D., J.D.

DEPUTY ADMINISTRATOR AND

DIRECTOR, CENTER FOR PROGRAM INTEGRITY

CENTERS FOR MEDICARE & MEDICAID SERVICES

ON

HARNESSING TECHNOLOGY AND INNOVATION TO CUT WASTE AND CURB FRAUD IN FEDERAL HEALTH PROGRAMS

BEFORE THE

UNITED STATES SENATE COMMITTEE ON HOMELAND SECURITY & GOVERNMENTAL AFFAIRS,

SUBCOMMITTEE ON FEDERAL FINANCIAL MANAGEMENT, GOVERNMENT INFORMATION, FEDERAL SERVICES, AND INTERNATIONAL SECURITY

JULY 12, 2011

U.S. Senate Committee on Homeland Security & Governmental Affairs
Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security

Hearing on "Harnessing Technology and Innovation to Cut Waste and Curb Fraud in Federal Health Programs"
July 12, 2011

Chairman Carper, Ranking Member Brown, and Members of the Subcommittee, thank you for the invitation to discuss how the Centers for Medicare & Medicaid Services' (CMS) advanced technological initiatives will draw on private sector experience to reduce fraud, waste, and abuse in Medicare, Medicaid, and the Children's Health Insurance Program (CHIP).

The Administration is committed to reducing fraud, waste, and improper payments. On June 13, 2011, President Obama launched the Campaign to Cut Waste, a campaign to find and eliminate misspent tax dollars in every agency and department across the Federal government.

Complementing that effort, on July 1, 2011, CMS implemented a new predictive modeling technology developed with private industry experts to fight Medicare fraud. Similar to the technology used by credit card companies, predictive modeling will help identify fraudulent Medicare claims prior to payment on a nationwide basis so we can begin to take action to stop fraudulent payments before they are made. This initiative builds on the new anti-fraud tools and resources provided by the Affordable Care Act. These tools include new screening and enrollment requirements, strengthened authority to suspend potentially fraudulent payments, and increased coordination of antifraud actions and policies between Medicare and Medicaid. Together, these tools are helping us move beyond "pay and chase" recovery operations to an approach that prevents fraud and abuse prior to providing payment.

Predictive Modeling

To combat health care fraud more effectively, CMS is developing new methods and technologies to get ahead of criminals and identify their patterns of behavior early. We have launched an ambitious national effort to stop criminals at every step of the claims process – by strengthening Medicare enrollment standards and processes, by making it harder for fraudsters to bill

Medicare, and now by seeking to uncover suspicious billing patterns that may indicate fraud. This is not easy, but it is a challenge this Administration is committed to meeting. Every workday, Medicare pays out more than $1 billion from 4.5 million claims, and is statutorily required to pay claims quickly, usually within 14 to 30 days. Preventing fraud in Medicare involves paying serious attention to an important balance: carrying out our core responsibility to protect beneficiary access to necessary health care services and to reduce the administrative burden on legitimate providers, while identifying and thoroughly investigating suspect claims and reducing fraud, waste, and abuse.

The new authorities given to us by Congress and the experience of private sector industries in combating fraud have greatly enhanced our capacity to carry out this task. We are now using predictive modeling technology to assign risk scores to Medicare claims, which can allow us to focus our investigative resources. Predictive modeling is an innovative technology that can detect potential fraud and abuse by simultaneously analyzing multiple data sources, such as provider billing patterns and the distance between service location and a beneficiary's address, for a very large number of claims. Many private industries use similar predictive models to protect against fraud. Our new system is able to identify suspect claims before we pay. Through this new technology, we now have an integrated view of fee-for-service Medicare claims nationwide, expanding our analysis beyond designated regions to reveal scams that may be operating across the country. This comprehensive view allows our investigators to see and analyze billing patterns as claims are submitted, instead of relying primarily on post-payment data.

Small Business Jobs Act Authorities

Nationwide Implementation of Predictive Modeling for Medicare Fee-for-Service

CMS is actively implementing the new tools and authorities given to us by Congress to reduce fraud, waste, and abuse. The Small Business Jobs Act of 2010 (P.L. 111-240) originally envisioned a phased-in approach for predictive modeling technology. I am pleased to report that we have implemented this provision aggressively and efficiently only nine months after the President signed the bill into law. In one important aspect, we are well ahead of the statutory schedule: instead of implementing predictive modeling in an initial ten States in the first

implementation year, as required by the statute, we applied the predictive modeling technology to Medicare fee-for-service claims nationwide on July 1, 2011. All claims across the country are now being screened before they are paid. The ones with the highest risk scores will receive immediate attention and additional review by our analysts through our new rapid response strategy. The rapid response strategy will permit us to examine the conduct that produced the high-risk score, and then to consider a wide variety of appropriate actions, including claim denial, payment suspension or revocation, as well as referral to law enforcement. We decided to implement the technology nationwide to maximize the benefit from predictive models as soon as possible. Nationwide implementation also helps CMS integrate the technology into the Medicare fee-for-service program efficiently across our Medicare Administrative Contractors and anti-fraud contractors. We will also evaluate the possibility of expanding predictive modeling to Medicaid and CHIP over the next few years.

Predictive Modeling Contracts

Through the competitive solicitation and award process, we selected Northrop Grumman, a global provider of advanced information solutions, to implement our predictive modeling technology. Northrop Grumman has built an integrated team with Federal Network Systems, a Verizon company, and National Government Services, a longtime Medicare payment contractor, to develop, refine, and implement the new system, incorporating best practices from both public and private stakeholders into a system unique to CMS' needs.

Our contractor, using proven predictive models and other advanced analytics, has moved rapidly to implement the new technology. We have deployed algorithms and an analytical process that look at Medicare claims – by beneficiary, provider, service origin, and other variables – to identify potential problems and assign an ~~"a~~lert" and ~~"r~~isk scores" for those claims. The new system alerts us to a potential problem, including unusual billing patterns or other suspicious behavior , while simultaneously prioritizing claims so we can strategically target our resources for additional review and investigation, as necessary.

The Small Business Jobs Act requires two contracts, and CMS is in the final stages of awarding the second one. As described above, the first award to the integrated team of three companies

implemented all of the elements of the predictive modeling requirements on July 1, 2011. The additional contract will be awarded to develop additional predictive analytic models that will complement the existing models already in place. These models will run concurrently on the system implemented by Northrop Grumman and its team.

The new system will expand and grow in sophistication over time. We have started by using a set of well-established algorithms and will refine, develop, and identify additional algorithms over the coming months and years. We will base the new algorithms on a variety of sources, such as law enforcement investigations, private sector experience, and the results of our own data analyses and investigations.

Additional Fraud Detection Efforts

CMS is also implementing other exciting initiatives including streamlining the new health care provider enrollment requirements authorized by the Affordable Care Act. Last week, we posted a solicitation limited to eligible 8(a) contractors or businesses that meet the criteria for Small Disadvantaged Business qualification and are certified with the Small Business Administration for an automated provider enrollment screening solution following the successful completion of a pilot. The pilot leveraged an external private sector database to test the added value of augmenting our internal data on provider enrollment with publicly available information on a rolling basis. CMS verifies and validates various data elements on provider enrollment applications using a multitude of websites available to the general public. This process of verification is somewhat cumbersome, and resource intensive. Additionally, maintaining provider data is currently dependent on providers self-reporting changes in information that is relevant to Medicare enrollment. When changes are not reported at all or are reported in an untimely manner, providers who are not or are no longer eligible for enrollment continue to bill the program. We found that linking an automated screening tool to our Medicare enrollment database significantly reduced the application processing time by providing ~~-~~one-stop shopping" for enrollment relevant information. Continuous, automated monitoring of the enrollment database identified outdated provider records more quickly, and permitted the proactive confirmation of key information changes. This provides us with another opportunity to save

taxpayer money, particularly in the area of monitoring license expiration, by timely identifying ineligible providers and taking appropriate actions to ensure they are not improperly billing.

We anticipate that this new screening technology will automatically verify information provided on an enrollment application for all Medicare provider and supplier types in all 50 States, the District of Columbia, and the five Territories. The screening will compile CMS data and appropriate external data sources, such as the National Plan and Provider Enumeration Systems for the National Provider Identifier (NPI), the General Services Administration (GSA) Excluded Parties List, and the Office of the Inspector General (OIG) exclusion database. The screening will also actively monitor compliance with requirements such as license status or changes in physical location. We anticipate completing the competitive procurement process this fall, with full implementation by the end of the year.

Collaborating with the States

We have implemented the Medicaid and CHIP State Information Sharing (MCSIS) system that provides data directly to the States regarding terminated providers. For providers who have been terminated from one State Medicaid or CHIP program, this system will prevent enrollment in another State program, protecting scarce Medicaid and CHIP dollars. Further, CMS will be sharing information on providers that have been terminated from Medicare for cause with the State programs as well. If one program knows, all HHS (Medicare, Medicaid, CHIP) health programs should know. This tool is the beginning of a smarter, more efficient Federal-State partnership, integrating technology solutions to routinely share relevant program information in a collaborative effort.

For the continuing education of State program integrity employees, the Medicaid Integrity Institute (MII) stands out as one of CMS's most significant achievements. The MII provides a unique opportunity for CMS to offer substantive training, technical assistance, and support to States in a structured learning environment. In its three years of existence, the MII has offered numerous courses and trained over 1,600 State employees at no cost to the States. Over time, the MII intends to create a credentialing process to elevate the professional qualifications of State Medicaid program integrity employees. As a result of the MII courses, State staff from across

the country have the opportunity to engage in productive dialogue about the challenges they face combating fraud, waste, and abuse issues unique to their State Medicaid programs. This interaction permits participants to share their success stories, to learn from other's successes, to give their Medicaid programs a wider range of perspectives on available policy options, and to help identify problem providers who attempt to migrate from one State Medicaid program to another.

Collaborating with the Private Sector

Building on the momentum generated by the National Health Care Fraud Summit in January 2010, CMS, in partnership with the Health and Human Services' OIG, the Department of Justice (DOJ), and the Administration on Aging, has convened regional health care fraud prevention summits across the country. These summits, held to date in Miami, Los Angeles, New York, Boston, Detroit, and Philadelphia, have brought together Federal and State officials, law enforcement experts, private insurers, beneficiaries, caregivers, and health care providers to discuss innovative ways to eliminate fraud within the nation's health care system. These summits also featured educational panels that discussed best practices for providers, beneficiaries, and law enforcement in preventing health care fraud. The panels included law enforcement officials, consumer experts, providers, and representatives of key government agencies. CMS continues to explore more opportunities to bring these stakeholder communities together in other cities to continue this important dialogue and strengthen our cooperative efforts across the Federal government and with the private sector.

CMS is also developing a process to share data on payment suspensions of providers and suppliers who provide services to Medicare patients with supplemental coverage from private plans. We are continuing to evaluate the possibility of sharing this data with all private plans.

Affordable Care Act Fraud-Fighting Tools

The Affordable Care Act is the most comprehensive legislative step forward to fight health care fraud in over a decade. The Act gives CMS and law enforcement officials tools they have never had before to protect Federal health care programs from fraud, waste, and abuse. It also provided $350 million in new program integrity resources, plus an inflation adjustment. With

this support, we are ramping up our anti-fraud efforts by increasing scrutiny of claims before we pay them, investing in sophisticated data analytics, and providing more ~~"~~boots on the ground" to fight health care fraud. Below I explain some of the tools that improve and enhance our efforts to prevent and detect fraud, and crack down on individuals who attempt health care fraud.

Enhanced Screening and Other Enrollment Requirements

On January 24, 2011, we announced a new rule (CMS-6028-FC) implementing a number of the Affordable Care Act's powerful new fraud prevention legislative tools. Under the rule, which took effect on March 25, 2011, CMS will conduct enhanced screening of categories of providers and suppliers that have historically posed a higher risk of fraud or abuse before they enroll in Medicare, Medicaid, or CHIP. The highest-risk categories of providers and suppliers, who will undergo the most extensive scrutiny, are newly enrolling suppliers of Durable Medical Equipment, Prosthetics, Orthotics and Supplies (DMEPOS) and home health agencies. The rule also establishes certain triggers that would move an individual provider or supplier into higher screening levels.

The enhanced screening established under the Affordable Care Act will generate a substantial number of unannounced site visits to providers and suppliers in the moderate and high-risk categories. Additionally, providers and suppliers who have been flagged through either predictive modeling or the automated enrollment screening will also undergo site visits to verify legitimacy. We anticipate that on-site inspections to validate or obtain information of record about different types of Medicare providers and suppliers will enhance our ability to follow up on suspect and high-risk providers. It will also help us efficiently meet the new site visit requirements for an expanded set of providers while reducing the time spent on site visits. To carry out a large number of site visits within very short timeframes, we have issued a request for information on our plan to consolidate site visit activities into one single national contract.

The rule also enforces the Secretary's new authority to impose a temporary moratorium on enrolling new providers or suppliers of a particular type in certain geographic areas, if that action is necessary to prevent or combat fraud, waste, and abuse. We plan to assess the impact of any proposed moratorium on beneficiary access, and we will publish a notice, including the rationale

for the moratorium, in the *Federal Register*. Importantly, the new rule implements the additional authority in the Affordable Care Act under which CMS, in consultation with the OIG, will suspend Medicare payments to providers or suppliers pending an investigation or final action on a credible allegation of fraud. The law has a parallel provision in the Medicaid program that requires States to withhold payments to Medicaid providers where there is a credible allegation of fraud. These tools will move Medicare and Medicaid beyond a ~~"p~~ay and chase" mode of having to track down fraudulent payments after the fact to one that prevents fraud before it occurs.

Increased Coordination of Fraud Prevention Efforts

Many of the Affordable Care Act provisions increase coordination between States, CMS, and our law enforcement partners at OIG and DOJ. By sharing information and requiring all States to terminate any provider or supplier that Medicare or another State terminated for cause, the law ensures that fraudulent providers and suppliers cannot easily move from State to State or between Medicare and Medicaid. We are also providing improved access to data and training in the use of data analytic systems to the OIG and DOJ, enabling investigators and law enforcement agents to more quickly detect and prosecute fraud schemes.

Collaborating with Law Enforcement Partners

CMS is committed to working with our law enforcement partners, who take a lead role in investigating and prosecuting alleged fraud. CMS provides support and resources to the Strike Forces, which investigate and track down individuals and entities defrauding Medicare and other government health care programs. Strike Force prosecutions are ~~"d~~ata driven" and target individuals and groups actively involved in ongoing fraud schemes. These efforts started in Miami in 2007and expanded to Los Angeles in 2008. In 2009 and 2010 under the HEAT initiative, we continued expanding the Strike Force to Detroit, Houston, Brooklyn, Tampa and Baton Rouge, and in 2011, the Strike Forces were expanded to Dallas and Chicago.

Sharing Data to Fight Fraud

The Affordable Care Act requires the centralization of certain claims data from Medicare, Medicaid and CHIP, the Department of Veterans Affairs, the Department of Defense, the Old-

Age, Survivors, and Disability Insurance program, and the Indian Health Service. Sharing data makes it easier for agency and law enforcement officials to coordinate and identify criminals and prevent fraud on a system-wide basis. Since 2006, CMS has been building the Integrated Data Repository (IDR), a data warehouse to integrate Medicare and Medicaid data so CMS and our partners can access data from a single source. The IDR will provide a comprehensive view of Medicare and Medicaid data including claims, beneficiary, and drug information. The IDR provides greater information sharing, broader and easier access to data, enhanced data integration, and increased security and privacy of data, while strengthening our analytical capabilities. The IDR makes fraud prevention and detection efforts more effective by eliminating duplicative efforts. It also provides a more rigorous source of data to help eliminate improper payments.

The IDR is currently populated with five years of historical Medicare Parts A, B, and D paid claims, and CMS is actively working to include pre-payment claims data. This additional data will allow us to analyze previously undetected indicators of aberrant activity throughout the claims process. We are also working to include the expanded set of data elements from States' Medicaid Management Information Systems that the Affordable Care Act requires States to report. This more robust State data set will be used alongside Medicare claims data in the IDR to detect potential fraud, waste, and abuse across multiple payers. Along with the IDR, the One Program Integrity (PI) web-based portal helps share data with our contractors and law enforcement. The portal provides a single access point to the data within the IDR, as well as analytic tools to review the data. CMS has been working closely with law enforcement to provide training and support in the use of One PI for their needs. These data initiatives will strengthen our program integrity work within State Medicaid programs and across CMS.

New Tools to Target High Risk Entities

As noted above, the Affordable Care Act strengthens the government's authority to require certain providers and suppliers program—based on the risk of fraud, waste, or abuse they pose—to undergo a higher level of scrutiny before enrolling in the Medicare program. Also, CMS issued rules on May 5, 2010 (CMS-6010-IFC) implementing Affordable Care Act provisions that require providers and suppliers who order and refer certain items or services for Medicare and

Medicaid beneficiaries to enroll in Medicare and Medicaid and maintain documentation on those orders and referrals. Finally, the Secretary may now require certain provider and suppliers to post a surety bond that is commensurate with the provider or supplier's volume of billing.

New Focus on Compliance and Prevention

Under the new law, providers and suppliers must establish compliance programs to ensure that they are aware of anti-fraud requirements and good governance practices and have incorporated those practices into their operations. Nursing homes are subject to new compliance and ethics plan requirements. Other preventive measures focus on certain categories of providers and suppliers that have a history of abuse, including Home Health agencies, DMEPOS suppliers, and Community Mental Health Centers (CMHCs). For example, on November 17, 2010, CMS finalized a rule (CMS-1510-F) implementing the Affordable Care Act requirement for patients to receive a ~~"~~face-to-face" visit with an appropriate health care professional when receiving Medicare home health and hospice services. Additionally, last week on July 5, 2011, CMS issued a proposed rule (CMS-2348-P) that aligns the Medicaid face-to-face requirements with the requirements in the Medicare programs. Another proposed rule implementing provisions in the Affordable Care Act was issued last week (CMS-1525-P). It requires CMHCs to provide at least 40 percent of their items and services to non-Medicare beneficiaries in order to prevent the creation of CMHCs solely for fraudulently billing Medicare.

Looking Forward

Medicare, Medicaid, and CHIP fraud affects every American by draining critical resources from our health care system, and contributes to the rising cost of health care for all. Taxpayer dollars lost to fraud, waste, and abuse harm multiple parties, particularly some of our most vulnerable citizens, not just the Federal government.

The Administration has made a firm commitment to rein in fraud and waste. With the new predictive modeling technology and Affordable Care Act provisions discussed today, we have more tools than ever before to move beyond ~~"~~pay and chase" and implement important strategic changes in pursuing fraud, waste, and abuse. Through partnerships between public and private

stakeholders, we have learned, from each other, how to better protect our health care system. I am confident that the harder we work today, the stronger our system will be for years to come.

I look forward to working with you in the future as we continue to make improvements in protecting the integrity of Federal health care programs and safeguarding taxpayer resources.

Testimony before the United States Senate

Committee on Homeland Security and Governmental Affairs

Subcommittee on Federal Financial Management

"Harnessing Technology and Innovation to Cut Waste and Curb Fraud in Federal Health Programs"

Testimony of:

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

July 12, 2011
2:30PM
342 Dirksen Senate Office Building

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

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

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

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

New Technologies Hold Tremendous Potential for Enhancing Our Fraud Fighting Efforts

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

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

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

U.S. Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security (July 12, 2011)

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

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

OIG's Use of Information Technology To Support Audits

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

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

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

U.S. Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security (July 12, 2011)

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

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

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

OIG Use of Information Technology in Support of Fraud Investigations

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

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

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

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

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

Use of Information Technology To Strengthen Program Integrity

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

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

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

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

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

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

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

Sharing Intelligence With Private Health Care Insurers

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

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

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

5

U.S. Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security (July 12, 2011)

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

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

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

Anticipating Vulnerabilities and Challenges Presented by the Use of Information Technology

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

These concerns are relevant across the spectrum of program integrity contractors we have reviewed, dating back to our 1998 findings of inconsistent performance among the Fiscal Intermediaries' fraud units that preceded Program Safeguard Contractors (PSC) and Zone Program Integrity Contractors.[5] Almost a decade later, in 2007, we found that PSCs also performed inconsistently, varying substantially in the number of new investigations initiated and cases referred to law enforcement, and producing minimal results in key areas such as proactive data analysis.[6] In a separate review, we found that CMS oversight of PSCs was lacking: evaluations of PSCs' performance did not include sufficient information and were not completed in time for evaluation results to be used in determining whether PSCs' contracts should be renewed.[7] More recently, a 2010 review of overpayments referred by PSCs found that just 2 of the 18 PSCs were responsible for 62 percent of the total amount of overpayments referred to claims processors for collection.[8] In the same 2010 review, we found that millions in overpayments identified by the PSCs were never collected.[9]

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

Conclusion

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

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

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

Thank you for the opportunity to testify.

10

U.S. Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security (July 12, 2011)

United States Government Accountability Office

GAO

Testimony
Before the Subcommittee on Federal Financial Management, Government Information, Federal Service, and International Security, Committee on Homeland Security and Government Affairs, U.S. Senate

For Release on Delivery
Expected at 2:30 p.m. EDT
Tuesday, July 12, 2011

FRAUD DETECTION SYSTEMS

Additional Actions Needed to Support Program Integrity Efforts at Centers for Medicare and Medicaid Services

Statement of Joel C. Willemssen,
Managing Director, Information Technology

GAO-11-822T

Mr. Chairman and Members of the Subcommittee:

I am pleased to participate in today's hearing on the Centers for Medicare and Medicaid Services' (CMS) efforts to protect the integrity of the Medicare and Medicaid programs, particularly through the use of information technology to help improve the detection of fraud, waste, and abuse in these programs. As you are aware, CMS is responsible for administering the Medicare and Medicaid programs[1] and leading efforts to reduce improper payments of claims for medical treatment, services, and equipment. Improper payments are overpayments or underpayments that should not have been made or were made in an incorrect amount; they may be due to errors, such as the inadvertent submission of duplicate claims for the same service, or misconduct, such as fraud or abuse. The Department of Health and Human Services reported about $70 billion in improper payments in the Medicare and Medicaid programs in fiscal year 2010.

Operating within the Department of Health and Human Services, CMS conducts reviews to prevent improper payments before claims are paid and to detect claims that were paid in error. These activities are predominantly carried out by contractors who, along with CMS personnel, use various information technology solutions to consolidate and analyze data to help identify the improper payment of claims. For example, these program integrity analysts may use software tools to access data about claims and then use those data to identify patterns of unusual activities by matching services with patients' diagnoses.

In 2006, CMS initiated activities to centralize and make more accessible the data needed to conduct these analyses and to improve the analytical tools available to its own and contractor analysts. At the Subcommittee's request, we have been reviewing two of these initiatives—the Integrated Data Repository (IDR), which is intended to provide a single source of data related to Medicare and Medicaid claims, and the One Program Integrity (One PI) system, a Web-based portal[2] and suite of analytical software tools used to extract data from IDR and enable complex analyses of these data. According to CMS officials responsible for

[1]Medicaid is a joint federal-state program for certain low-income individuals.

[2]The One PI portal is a Web-based user interface that enables a single login through centralized, role-based access to the system.

developing and implementing IDR and One PI, the agency had spent approximately $161 million on these initiatives by the end of fiscal year 2010.

My testimony, in conjunction with a report that we are releasing today,[3] summarizes the results of our study—which specifically assessed the extent to which IDR and One PI have been developed and implemented and CMS's progress toward achieving its goals and objectives for using these systems to detect fraud, waste, and abuse. All work on which this testimony is based was conducted at CMS's headquarters in Baltimore, Maryland, between June 2010 and July 2011, 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 provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Like financial institutions, credit card companies, telecommunications firms, and other private sector companies that take steps to protect customers' accounts, CMS uses information technology to help detect cases of improper claims and payments. For more than a decade, the agency and its contractors have used automated software tools to analyze data from various sources to detect patterns of unusual activities or financial transactions that indicate payments could have been made for fraudulent charges or improper payments. For example, to identify unusual billing patterns and support investigations and prosecutions of cases, analysts and investigators access information about key actions taken to process claims as they are filed and the specific details about claims already paid. This would include information on claims as they are billed, adjusted, and paid or denied; check numbers on payments of claims; and other specific information that could help establish provider intent.

CMS uses many different means to store and manipulate data and, since the establishment of the agency's program integrity initiatives in the

[3]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).

1990s, has built multiple, disparate databases and analytical software tools to meet the individual and unique needs of various programs within the agency. In addition, data on Medicaid claims are stored by the states in multiple systems and databases, and are not readily available to CMS. According to agency program documentation, these geographically distributed, regional approaches to data storage result in duplicate data and limit the agency's ability to conduct analyses of data on a nationwide basis. As a result, CMS has been working for most of the past decade to consolidate its databases and analytical tools.

CMS's Initiative to Develop a Centralized Source of Medicare and Medicaid Data

In 2006, CMS officials expanded the scope of a 3-year-old data modernization strategy to not only modernize data storage technology, but also to integrate Medicare and Medicaid data into a centralized repository so that CMS and its partners could access the data from a single source. They called the expanded program IDR.

According to program officials, the agency's vision was for IDR to become the single repository for CMS's data and enable data analysis within and across programs. Specifically, this repository was to establish the infrastructure for storing data related to Medicaid and Medicare Parts A, B, and D claims processing,[4] as well as a variety of other agency functions, such as program management, research, analytics, and business intelligence.

CMS envisioned an incremental approach to incorporating data into IDR. Specifically, it intended to incorporate data related to paid claims for all Medicare Part D data by the end of fiscal year 2006, and for Medicare Parts A and B data by the end of fiscal year 2007. The agency also planned to begin to incrementally add all Medicaid data for the 50 states in fiscal year 2009 and to complete this effort by the end of fiscal year 2012.

Initial program plans and schedules also included the incorporation of additional data from legacy CMS claims-processing systems that store

[4]Medicare Part A provides payment for inpatient hospital, skilled nursing facility, some home health, and hospice services, while Part B pays for hospital outpatient, physician, some home health, durable medical equipment, and preventive services. Further, all Medicare beneficiaries may purchase coverage for outpatient prescription drugs under Medicare Part D.

and process data related to the entry, correction, and adjustment of claims as they are being processed, along with detailed financial data related to paid claims. According to program officials, these data, called "shared systems" data, are needed to support the agency's plans to incorporate tools to conduct predictive analysis of claims as they are being processed, helping to prevent improper payments. Shared systems data, such as check numbers and amounts related to claims that have been paid, are also needed by law enforcement agencies to help with fraud investigations. CMS initially planned to have all the shared systems data included in IDR by July 2008.

CMS's Initiative to Develop and Implement Analytical Tools for Detecting Fraud, Waste, and Abuse

Also in 2006, CMS initiated the One PI program with the intention of developing and implementing a portal and software tools that would enable access to and analysis of claims, provider, and beneficiary data from a centralized source. The agency's goal for One PI was to support the needs of a broad program integrity user community, including agency program integrity personnel and contractors who analyze Medicare claims data, along with state agencies that monitor Medicaid claims. To achieve its goal, agency officials planned to implement a tool set that would provide a single source of information to enable consistent, reliable, and timely analyses and improve the agency's ability to detect fraud, waste, and abuse. These tools were to be used to gather data from IDR about beneficiaries, providers, and procedures and, combined with other data, find billing aberrancies or outliers. For example, an analyst could use software tools to identify potentially fraudulent trends in ambulance services by gathering the data about claims for ambulance services and medical treatments, and then use other software to determine associations between the two types of services. If the analyst found claims for ambulance travel costs but no corresponding claims for medical treatment, it might indicate that further investigation could prove that the billings for those services were fraudulent.

According to agency program planning documentation, the One PI system was also to be developed incrementally to provide access to IDR data, analytical tools, and portal functionality. CMS planned to implement the One PI portal and two analytical tools for use by program integrity analysts on a widespread basis by the end of fiscal year 2009. The agency engaged contractors to develop the system.

IDR and One PI Are in Use, but Lack Data and Functionality Essential to CMS's Program Integrity Efforts

IDR has been in use by CMS and contractor program integrity analysts since September 2006 and currently incorporates data related to claims for reimbursement of services under Medicare Parts A, B, and D. According to program officials, the integration of these data into IDR established a centralized source of data previously accessed from multiple disparate system files.

However, although the agency has been incorporating data from various sources since 2006, IDR does not yet include all the data that were planned to be incorporated by the end of 2010 and that are needed to support enhanced program integrity initiatives. Specifically, although initial program integrity requirements included the incorporation of the shared systems data by July 2008, these data have not yet been added to IDR. As such, analysts are not able to access certain data from IDR that would help them identify and prevent payment of fraudulent claims. According to IDR program officials, the shared systems data were not incorporated as planned because funding for the development of the software and acquisition of the hardware needed to meet this requirement was not approved until the summer of 2010. Since then, IDR program officials have developed project plans and identified user requirements, and told us that they plan to incorporate shared systems data by November 2011.

In addition, IDR does not yet include the Medicaid data that are critical to analysts' ability to detect fraud, waste, and abuse in this program. While program officials initially planned to incorporate 20 states' Medicaid data into IDR by the end of fiscal year 2010, the agency had not incorporated any of these data into the repository as of May 25, 2011. Program officials told us that the original plans and schedules for obtaining Medicaid data did not account for the lack of funding for states to provide Medicaid data to CMS, or the variations in the types and formats of data stored in disparate state Medicaid systems. Consequently, the officials were not able to collect the data from the states as easily as they expected and did not complete this activity as originally planned.

In December 2009, CMS initiated another agencywide program intended to, among other things, identify ways to collect Medicaid data from the many disparate state systems and incorporate the data into a single data store. As envisioned by CMS, this program, the Medicaid and Children's Health Insurance Program Business Information and Solutions (MACBIS) program, is to include activities in addition to providing expedited access to current data from state Medicaid programs. According to agency planning documentation, as a result of efforts to be initiated under the MACBIS program, CMS expects to incorporate Medicaid data for all 50

states into IDR by the end of fiscal year 2014. This enterprisewide initiative is expected to cost about $400 million through fiscal year 2016.

However, program officials have not defined plans and reliable schedules for incorporating the additional data into IDR that are needed to support the agency's program integrity goals. Yet, doing so is essential to ensuring that CMS does not repeat mistakes of the past that stand to jeopardize the overall success of its current efforts. In this regard, more than a decade ago, we reported on the agency's efforts to replace multiple claims processing systems with a single, unified system.[5] Among other things, that system was intended to provide an integrated database to help the agency in identifying fraud and abuse. However, as the system was being developed, we reported repeatedly that the agency was not applying effective investment management practices to its planning and management of the project. Further, we reported that the agency had no assurance that the project would be cost-effective, delivered within estimated timeframes, or even improve the processing of Medicare claims. Lacking these vital project management elements, CMS subsequently halted that troubled initiative without delivering the intended system—after investing more than $80 million over 3-and-a-half years.

Until the agency defines plans and reliable schedules for incorporating the additional data into IDR, it cannot ensure that current development, implementation, and deployment efforts will provide the data and technical capabilities needed to enhance CMS's efforts to detect potential cases of fraud, waste, and abuse.

Beyond the IDR initiative, CMS program integrity officials have not yet taken appropriate actions to ensure the use of One PI on a widespread basis for program integrity purposes. According to program officials, the system was deployed in September 2009 as originally planned and consisted of a portal that provided Web-based access to software tools used by CMS and contractor analysts to retrieve and analyze data stored in IDR. As currently implemented, the system provides access to two analytical tools. One tool is a commercial off-the-shelf decision support tool that is used to perform data analysis to, for example, detect patterns

[5]GAO, *Medicare Automated Systems: Weaknesses in Managing Information Technology Hinder Fight Against Fraud and Abuse,* GAO/T-AIMD-97-176 (Washington, D.C.: September 29, 1997). At the time of this report, CMS was known as the Health Care Financing Administration.

of activities that may identify or confirm suspected cases of fraud, waste, or abuse. The second tool provides users with extended capabilities to perform more complex analyses of data. For example, it allows the user to customize and create ad hoc queries of claims data across the different parts of the Medicare program.

However, while program officials deployed the One PI portal and two analytical tools, the system is not being used as widely as planned because CMS and contractor analysts have not received the necessary training for its use. In this regard, program planning documentation from August 2009 indicated that One PI program officials had planned for 639 analysts to be trained and using the system by the end of fiscal year 2010; however, CMS confirmed that by the end of October 2010, only 42 of those intended users had been trained to use One PI, with 41 actively using the portal and tools. These users represent fewer than 7 percent of the users originally intended for the program.

Program officials responsible for implementing the system acknowledged that their initial training plans and efforts had been insufficient and that they had consequently initiated activities and redirected resources to redesign the One PI training plan in April 2010; they began to implement the new training program in July of that year. As of May 25, 2011, One PI officials told us that 62 additional analysts had signed up to be trained in 2011 and that the number of training classes for One PI had been increased from two to four per month. Agency officials, in commenting on our report, stated that since January 2011, 58 new users had been trained; however, they did not identify an increase in the number of actual users of the system.

Nonetheless, while these activities indicate some progress toward increasing the number of One PI users, the number of users expected to be trained and to begin using the system represents a small fraction of the population of 639 intended users. Moreover, as of late May 2011, One PI program officials had not yet made detailed plans and developed schedules for completing training of all the intended users. Agency officials concurred with our conclusion that CMS needs to take more aggressive steps to ensure that its broad community of analysts is trained. Until it does so, the use of One PI may remain limited to a much smaller group of users than the agency intended, and CMS will continue to face obstacles in its efforts to deploy One PI for widespread use throughout its community of program integrity analysts.

CMS Is Not Yet Positioned to Identify Financial Benefits or to Fully Meet Program Integrity Goals and Objectives through the Use of IDR and One PI

Because IDR and One PI are not being used as planned, CMS officials are not yet in a position to determine the extent to which the systems are providing financial benefits or supporting the agency's initiatives to meet program integrity goals and objectives. As we have reported, agencies should forecast expected benefits and then measure actual financial benefits accrued through the implementation of information technology programs.[6] Further, the Office of Management and Budget (OMB) requires agencies to report progress against performance measures and targets for meeting them that reflect the goals and objectives of the programs.[7] To do this, performance measures should be outcome-based and developed with stakeholder input, and program performance must be monitored, measured, and compared to expected results so that agency officials are able to determine the extent to which goals and objectives are being met. In addition, industry experts describe the need for performance measures to be developed with stakeholders' input early in a project's planning process to provide a central management and planning tool and to monitor the performance of the project against plans and stakeholders' needs.

While CMS has shown some progress toward meeting the programs' goals of providing a centralized data repository and enhanced analytical capabilities for detecting improper payments due to fraud, waste, and abuse, the current implementation of IDR and One PI does not position the agency to identify, measure, and track financial benefits realized from reductions in improper payments as a result of the implementation of either system. For example, program officials stated that they had developed estimates of financial benefits expected to be realized through the use of IDR. The most recent projection of total financial benefits was reported to be $187 million, based on estimates of the amount of improper payments the agency expected to recover as a result of analyzing data provided by IDR. With estimated life-cycle program costs of $90 million through fiscal year 2018, the resulting net benefit expected from implementing IDR was projected to be $97 million. However, as of

[6]GAO, *Secure Border Initiative: DHS Needs to Reconsider Its Proposed Investment in Key Technology Program*, GAO-10-340 (Washington, D.C.: May 5, 2010) and *DOD Business Systems Modernization: Planned Investment in Navy Program to Create Cashless Shipboard Environment Needs to be Justified and Better Managed*, GAO-08-922 (Washington, D.C.,: Sept. 8, 2008).

[7]OMB, *Guide to the Performance Assessment Rating Tool.*

March 2011, program officials had not identified actual financial benefits of implementing IDR.

Further, program officials' projection of financial benefits expected as a result of implementing One PI was most recently reported to be approximately $21 billion. This estimate was increased from initial expectations based on assumptions that accelerated plans to integrate Medicare and Medicaid data into IDR would enable One PI users to identify increasing numbers of improper payments sooner than previously estimated, thus allowing the agency to recover more funds that have been lost due to payment errors.

However, the current implementation of One PI has not yet produced outcomes that position the agency to identify or measure financial benefits. CMS officials stated at the end of fiscal year 2010—more than a year after deploying One PI—that it was too early to determine whether the program has provided any financial benefits. They explained that, since the program had not met its goal for widespread use of One PI, there were not enough data available to quantify financial benefits attributable to the use of the system. These officials said that as the user community is expanded, they expect to be able to begin to identify and measure financial and other benefits of using the system.

In addition, program officials have not developed and tracked outcome-based performance measures to help ensure that efforts to implement One PI and IDR meet the agency's goals and objectives for improving the results of its program integrity initiatives. For example, outcome-based measures for the programs would indicate improvements to the agency's ability to recover funds lost because of improper payments of fraudulent claims. However, while program officials defined and reported to OMB performance targets for IDR related to some of the program's goals, they do not reflect the goal of the program to provide a single source of Medicare and Medicaid data that supports enhanced program integrity efforts. Additionally, CMS officials have not developed quantifiable measures for meeting the One PI program's goals. For example, performance measures and targets for One PI include increases in the detection of improper payments for Medicare Parts A and B claims. However, the limited use of the system has not generated enough data to quantify the amount of funds recovered from improper payments.

Because it lacks meaningful outcome-based performance measures and sufficient data for tracking progress toward meeting performance targets, CMS does not have the information needed to ensure that the systems

are useful to the extent that benefits realized from their implementation help the agency meet program integrity goals. Further, until CMS is better positioned to identify and measure financial benefits and establishes outcome-based performance measures to help gauge progress toward meeting program integrity goals, it cannot be assured that the systems will contribute to improvements in CMS's ability to detect fraud, waste, and abuse in the Medicare and Medicaid programs, and prevent or recover billions of dollars lost to improper payments of claims.

Given the critical need for CMS to improve the management of and reduce improper payments within the Medicare and Medicaid programs, our report being released today recommends a number of actions that we consider vital to helping CMS achieve more widespread use of IDR and One PI for program integrity purposes. Specifically, we are recommending that the Administrator of CMS

- finalize plans and develop schedules for incorporating additional data into IDR that identify all resources and activities needed to complete tasks and that consider risks and obstacles to the IDR program;
- implement and manage plans for incorporating data in IDR to meet schedule milestones;
- establish plans and reliable schedules for training all program integrity analysts intended to use One PI;
- establish and communicate deadlines for program integrity contractors to complete training and use One PI in their work;
- conduct training in accordance with plans and established deadlines to ensure schedules are met and program integrity contractors are trained and able to meet requirements for using One PI;
- define any measurable financial benefits expected from the implementation of IDR and One PI; and
- with stakeholder input, establish measurable, outcome-based performance measures for IDR and One PI that gauge progress toward meeting program goals.

- In commenting on a draft of our report, CMS agreed with these recommendations and indicated that it plans to take steps to address the challenges and problems that we identified during our study.

In summary, CMS's success toward meeting its goals to enhance program integrity will depend upon the agency's incorporation of all needed data into IDR as well as the effective use of the systems by the agency's broad community of program integrity analysts. In addition, a vital step will be the identification of measurable financial benefits and performance goals expected to be attained through improvements in the agency's ability to prevent and detect fraudulent, wasteful, and abusive claims and resulting improper payments. In taking these steps, the agency will better position itself to determine whether these systems are useful for enhancing CMS's ability to identify fraud, waste, and abuse and, consequently, reduce the loss of funds resulting from improper payments of Medicare and Medicaid claims.

Mr. Chairman, this concludes my prepared statement. I would be pleased to answer any questions you or other Members of the Subcommittee may have.

GAO Contacts and Staff Acknowledgments

If you have questions concerning this statement, please contact Joel C. Willemssen, Managing Director, Information Technology Team, at (202) 512-6253 or willemssenj@gao.gov; or Valerie C. Melvin, Director, Information Management and Human Capital Issues, at (202) 512-6304 or melvinv@gao.gov. Other individuals who made key contributions include Teresa F. Tucker (Assistant Director), Sheila K. Avruch (Assistant Director), April W. Brantley, Clayton Brisson, Neil J. Doherty, Amanda C. Gill, Nancy Glover, Kendrick M. Johnson, Lee A. McCracken, Terry L. Richardson, Karen A. Richey, and Stacey L. Steele.

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 Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to 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 Web site, 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.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact: Web site: www.gao.gov/fraudnet/fraudnet.htm E-mail: fraudnet@gao.gov Automated answering system: (800) 424-5454 or (202) 512-7470
Congressional Relations	Ralph Dawn, Managing Director, dawnr@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

Statement of Louis Saccoccio

Executive Director

National Health Care Anti-Fraud Association

"Can New Technology and Private Sector Business Practices Cut Waste and Fraud in Medicare and Medicaid?"

Before the

U.S. Senate Committee on

Homeland Security & Governmental Affairs

Subcommittee on Federal Financial Management, Government Information, Federal Services, & International Security

July 12, 2011

NHCAA
National Health Care Anti-Fraud Association

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

Good afternoon, Chairman Carper, Ranking Member Brown and other distinguished Members of the Subcommittee. I am Louis Saccoccio, Executive Director 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. We are uncommon among associations in that we are a private-public partnership—our members comprise more than 85 of the nation's most prominent private health insurers, along with more than 85 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 simple: 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. The magnitude of this mission remains the same regardless of whether a patient has private health coverage as an individual or through an employer, or is covered by a public program such as Medicare, Medicaid, or TRICARE.

I am grateful for the opportunity to discuss the problem of health care fraud with you. In my testimony today, I draw upon our organization's 25-plus years of experience focusing on this single issue. Health care fraud is a serious and costly problem that affects every patient and every taxpayer in America. The financial losses due to health care fraud are estimated to range from $75 billion to a staggering $250 billion a year. These financial losses are compounded by numerous instances of patient harm—unfortunate and insidious side effects of health care fraud.

NHCAA
National Health Care Anti-Fraud Association

Health care fraud is an exceptionally complex crime that manifests in countless ways. There are many variables at play. Considering that billions of medical claims are generated in the United States every year, the sheer volume of health care claims makes fraud detection a challenge. Medicare alone pays 4.4 million claims per day to 1.5 million providers nationwide. Anyone in the system can conceivably commit fraud, and those committing fraud have the full range of medical conditions and treatments and the entire population of patients on which to base false claims. Detecting health care fraud often requires the knowledge and application of clinical best practices, as well as knowledge of medical terminology and specialized coding systems, including CPT and CDT codes, DRGs, ICD-9 codes, and the forthcoming ICD-10 codes. Clearly, health care fraud can be a challenging crime to prevent and detect. The perpetrators of this crime have proven themselves to be creative, nimble and aggressive. Therefore, investing in and employing the most effective fraud prevention and detection techniques is critical to achieving success.

Beyond the monetary losses, health care fraud is a crime that directly affects the quality of health care delivery. Patients are physically and emotionally harmed by health care fraud. The perpetrators of some types of health care fraud schemes deliberately and callously place trusting patients at significant risk of injury or even death. While distressing to imagine, there are cases where patients have been subjected to unnecessary, dangerous and invasive medical procedures simply because of greed. Consequently, fighting health care fraud is not only a financial necessity; it is a patient safety imperative. Anti-fraud efforts identify and prevent unnecessary and potentially harmful medical care and procedures.

Additionally, anti-fraud efforts identify dangerous prescription drug abuse by patients, overprescribing by some physicians, and involvement by some pharmacists who are complicit in the scheme. Prescription drug abuse is a growing problem. Addicts will go "doctor shopping" in order to get multiple prescriptions from several physicians and will then fill them at different pharmacies. Often, it's the insurer who is best able to connect the dots and identify overprescribing by physicians and prescription drug abuse by patients. NHCAA also sees promise in state prescription drug monitoring programs as a means to not only identify fraud but

to protect patients. Encouraging state investments in these monitoring programs through incentives is a worthwhile consideration, as is examining interoperability among state programs. Useful insights about drug diversion and other pharmacy-related fraud trends could likely be identified if the ability to compare or consider monitoring program data across multiple states were formalized.

Health care anti-fraud efforts also identify and help prevent medical identity theft. Using a person's name or other identifying information without that person's knowledge or consent to obtain medical services, or to submit false insurance claims for payment, constitutes medical identity theft. It can result in erroneous information being added to a person's medical record or the creation of a fictitious medical record in the victim's name. These victims could receive the wrong (and potentially harmful) medical treatment, find that their health insurance benefits have been exhausted, become uninsurable for life insurance coverage, or have their ability to obtain employment impacted. Untangling the web of deceit spun by perpetrators of medical identity theft can be a grueling and stressful endeavor, and the effects of this crime can plague a victim's medical and financial status for years to come. And medical identity theft is not a crime limited to patients—with increasing regularity, health care providers are finding themselves victims of identity theft too, often resulting in serious damage to their professional reputations.

My testimony today will focus on three issues which NHCAA believes are critical to successfully combat health care fraud. The first is the importance of anti-fraud information sharing among all payers of health care, including the sharing of information between private insurers and public programs. The second is the critical role of data consolidation and data analytics in being able to prevent precious health care dollars from being lost to fraud. Finally, I will address the value of new anti-fraud tools provided by recent legislation, including the Affordable Care Act (ACA) and the Small Business Jobs and Credit Act of 2010, and the need to build upon these new tools to ensure continued and consequential private and public investment in anti-fraud efforts.

NHCAA
National Health Care Anti-Fraud Association®

I. The sharing of anti-fraud information among all payers – government programs and private insurers alike — is crucial to successfully fighting health care fraud and should be encouraged and enhanced.

Health care fraud does not discriminate between types of medical coverage. The same schemes used to defraud Medicare migrate over to private insurers, 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.

NHCAA has stood as an example of the power of a private-public partnership against health care fraud since its founding, and we believe that health care fraud should be addressed with private-public solutions. 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 works in combating health care fraud, and NHCAA dedicates itself to providing venues in which the sharing of relevant information can take place.

For example, NHCAA hosts several anti-fraud information-sharing meetings each year in which private health plans and representatives of the FBI, the Investigations Division of HHS-OIG, State Medicaid Fraud Control Units, TRICARE, and other federal and state agencies come together to share information about emergent fraud schemes and trends. Moreover, NHCAA's Request for Investigation Assistance (RIA) process allows government agents to easily query private health insurers regarding their financial exposure in active health care fraud cases. For the past decade, NHCAA has conducted a biennial survey of its private-sector members that aims to assess the structure, staffing, funding, operations and results of health insurer investigative units. In the most recent survey report (with data collected in 2009), 100% of respondents reported that they responded to NHCAA Requests for Investigation Assistance from

law enforcement. Earlier this year, an FBI special agent who had submitted an RIA provided NHCAA feedback regarding the value of the process, stating that an estimated $1.5 million in additional fraud dollars were identified as a result. The special agent rated the RIA process as "Excellent."

In addition to the NHCAA-sponsored information-sharing forums, many U.S. Attorney Offices sponsor health care fraud task forces that hold routine meetings. In the same survey mentioned above, 89 percent of NHCAA private insurer members stated that they have shared case information at law enforcement-sponsored health care fraud task force meetings.[1] It is clear that private insurers regularly share information with law enforcement, which in turn aids ongoing investigations.

The Department of Justice (DOJ) has 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.[2] Likewise, CMS has recognized the value of greater information sharing. During a September 22, 2010 Congressional subcommittee hearing, Peter Budetti, M.D., J.D., Deputy Administrator and Director of the Center for Program Integrity, stated: "Sharing information and performance metrics broadly and engaging internal and external stakeholders involves establishing new partnerships with government and private sector groups. Because the public and private sectors have common challenges in fighting fraud and keeping fraudulent providers at bay, it makes sense that we should join together in seeking common solutions."

In Philadelphia this past June, the Department of Health and Human Services (HHS) and the Department of Justice (DOJ) co-hosted their sixth regional Health Care Fraud Prevention

[1] NHCAA Anti-Fraud Management Survey for Calendar Year 2009, National Health Care Anti-Fraud Association, June 2010.
[2] See http://www.usdoj.gov/ag/readingroom/hcarefraud2.htm.

Summit. The importance and promise of partnership in fighting health care fraud emerged as a major theme of the event. Attorney General Eric Holder offered keynote remarks highlighting the value of information sharing and collaboration in tackling health care fraud: "When it comes to addressing a challenge as urgent, as complex, and as widespread as health care fraud, we need an innovative, proactive, and collaborative approach...There's no question that we need strong public-private partnerships."[3] Further asserting his commitment to this idea, Attorney General Holder said, "[The DOJ] will continue to engage key stakeholders in the private sector in our anti-fraud efforts...As we move forward, we will seek out guidance from representatives of the insurance industry and in the health care-provider community."

Likewise, in her keynote remarks, HHS Secretary Kathleen Sebelius described the Summit as "an important opportunity to build partnerships between public and private stakeholders who are invested in our fight against health care fraud. We have already begun to develop the relationships that can form the foundation for long-term cooperation."[4]

The Summit agenda was designed to showcase private-public partnerships against fraud that have yielded success. For example, one panel discussion was based on the *United States of America v. Stephen J. Schneider, D.O and Linda K. Schneider, L.P.N.* case, the prosecution of which was honored with the NHCAA 2010 Investigation of the Year Award. This four-year investigation into the operation of a pain management clinic in a small community south of Wichita, Kansas involved extensive over-prescribing of controlled substances, resulting in more than 100 drug overdoses, with the deaths of at least 68 persons linked to the case. The far-reaching investigative team included federal, state and private-sector representatives, offering a perfect illustration of the efficacy of private-public partnership.

Another example that illustrates the power of cooperative efforts against health care fraud can be found in South Florida, viewed by many as the epicenter for emerging fraud schemes. Here, "phantom" health care providers, which do not exist except on paper, yet manage to defraud

[3] See http://www.justice.gov/iso/opa/ag/speeches/2011/ag-speech-110617.html
[4] See http://www.hhs.gov/secretary/about/speeches/sp20110617.html

public and private programs of millions of dollars, had become an acute problem over the last several years.

One effort by HHS-OIG in 2007 to validate durable medical equipment, prosthetics, orthotics, and supply (DMEPOS) providers under Medicare revealed that nearly one third – 491 – of the 1,581 DME providers in three South Florida counties simply did not exist.[5] These phantom providers had collected hundreds of millions of dollars from Medicare, Medicaid and other public programs. As a result of this type of wide-spread fraud, the Department of Justice organized its first Health Care Fraud Strike Force in Miami-Dade County.[6]

While the government-led Strike Force was investigating, significant intelligence about these phantom providers was also being developed by private health insurers, much of it driven by information provided by beneficiaries – individuals who received Explanation of Benefit forms for services they had not received. Once information began to be shared between the public and private sectors, NHCAA member company investigators were able to review beneficiary information to determine that the same Social Security numbers were being used repeatedly by these phantom providers. A search of claim histories showed short, intense billing cycles by these providers, billing numerous services within a week or two. When investigators tried to contact these alleged providers by telephone, they typically found disconnected numbers or full voicemail boxes. Messages that were left by investigators were never returned.

In response to the challenge of phantom providers and other health care fraud schemes in South Florida, including fraud schemes involving infusion therapy and home health care, NHCAA formed a South Florida Work Group. In meetings held in 2009 and 2010, this NHCAA work group brought together representatives of private insurers, FBI headquarters and 10 FBI field divisions, the Centers for Medicare and Medicaid Services (CMS), the Department of Health and Human Services Office of Inspector General (HHS-OIG), the Justice Department, the Miami U.S. Attorney's Office, the Office of Personnel Management Office of Inspector General (OPM-

[5] See http://oig.hhs.gov/publications/docs/press/2007/PRSouthFlorida.pdf.
[6] See http://www.stopmedicarefraud.gov/heatsuccess/heat_taskforce_miami.pdf.

OIG), the Department of Defense (DOD) TRICARE, and local law enforcement to address the health care fraud schemes emerging from South Florida. The details of these schemes, the investigatory tactics, and the results of recent prosecutions were discussed with the dual goals of preventing additional losses in South Florida and preventing the schemes from spreading and taking hold in other parts of the nation.

Despite how information sharing has progressed between the private and public payers of health care, on occasion some federal and state agents have been under the misapprehension that they do not have the authority to share information about health care fraud with private insurers, creating an unnecessary yet significant obstacle in coordinated fraud fighting efforts. It would greatly enhance the fight against health care fraud if federal and state agencies clearly communicate with their agents the guidelines for sharing information with private insurers, emphasizing that information sharing for the purposes of preventing, detecting and investigating health care fraud is authorized, encouraged and consistent with applicable legal principles. NHCAA is working closely with the HHS-OIG, CMS, and DOJ to identify the barriers, both actual and perceived, to more effective anti-fraud information sharing with the goal of increasing the effectiveness of this critical tool in the fight against health care fraud.

We understand that Senate Bill 1251, the anti-fraud measure recently introduced by Senators Carper and Coburn, includes several provisions that promote expanded data sharing. The bill describes a plan to permit Medicare program safeguard contractors (PSCs) and "other oversight contractors" such as Zone Program Integrity Contractors (ZPICs), Recovery Audit Contractors (RACs) and the special investigations units of Medicare contractors access to relevant government data as a means to improve fraud fighting. The legislation also includes a provision to expand access to the integrated data repository (IDR) established under the Affordable Care Act to "relevant State agencies," including state Medicaid plans, CHIP plans and Medicaid Fraud Control Units.

Sharing information and data with contractors of federal health programs and with state health programs is crucial to the success of anti-fraud efforts. Consistent with this concept, we also

would urge that, as CMS and the HHS-OIG move forward with data consolidation and analytics, the information developed from Medicare and Medicaid data on emerging fraud schemes and trends and their geographic locations be shared with private insurers to ensure the most effective and comprehensive focusing of anti-fraud resources, and to enhance the private-public partnership against health care fraud.

II. Data aggregation and analysis are essential tools in health care fraud detection and prevention.

The numbers are staggering: The U.S. health care system spends $2.5 trillion dollars and generates billions of claims a year from hundreds of thousands 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 claims for potential fraud, each payer is limited to the claims it receives and adjudicates. There is no single repository of health care claims similar to what exists for property and casualty insurance claims.[7] The complexity and size of the health care system, along with understandable concerns for patient privacy, probably make such a database impracticable. This fact further emphasizes the importance of anti-fraud information sharing among all payers of health care.

Nevertheless, data consolidation is possible at some level. NHCAA is encouraged by the expanded data matching provisions provided for in Section 6402(a) of the Affordable Care Act. This section mandates an expanded "Integrated Data Repository" at CMS that will incorporate data from all federal health care programs. The law stipulates that inclusion of Medicare data into the Integrated Data Repository "shall be a priority," and data from the other federal programs shall be included "as appropriate." As a result, this provision establishes the *ability* to create an "all claims" database, albeit limited to government programs, with the purpose of

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

conducting law enforcement and oversight activities. This is a major step in the right direction for analyzing claims data in a way that will stem potential losses and identify emerging schemes at the earliest possible time.

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 detect emerging fraud patterns and schemes in a timely manner is to aggregate claims data as much as practicable, then apply cutting-edge technology to the data to detect risks and emerging fraud trends. 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.

In recognition of this fact, some commercial health insurers have begun to utilize, or are in the process of evaluating the use of, predictive analytics, applying them to fraud prevention efforts on the front end, prior to medical claims being paid. This is similar to the technology that credit card companies and financial institutions use to detect and prevent fraud. It works by searching vast amounts of data and applying risk-scoring and building models based on patterns that emerge from that data. At the June Fraud Prevention Summit in Philadelphia, Jeff Brewer of technology company FICO participated in a panel that discussed the use of technology and data sharing among private and public payers. FICO, an NHCAA member, has extensive experience in applying predictive modeling techniques to the financial services industry and is now applying these technologies to health care, with clients such as Highmark Blue Cross Blue Shield in Pennsylvania. Mr. Brewer explained that within a payer organization, there are many stakeholders and real-time data analytics solutions really must work as "enterprise-wide systems." In estimating the promise that data analytics holds for health care, he stated, "FICO technology works in real-time—by milliseconds—for your credit card. We hope to get health care there. The technology is there."

The federal government has also recognized the value of data analysis as a key aspect of its inter-agency HEAT initiative. The Health Care Fraud Prevention and Enforcement Action Team (HEAT) counts among its goals improved data sharing—including access to real-time data—to

detect fraud patterns, and strengthened partnerships between the public and private health sectors. The Medicare Strike Force model employed by the HEAT program combines all Medicare paid claims into a single, searchable database, identifying potential fraud more quickly and effectively. There are currently Strike Force teams operating in nine metro centers across the country. The Strike Forces' use of improved real time data access and analysis has resulted in more than 520 successful prosecutions and 465 indictments involving charges filed against 829 defendants over the last four years.[8]

Congress has demonstrated its commitment to combating fraud by applying predictive modeling techniques to health care anti-fraud efforts through the Small Business Jobs and Credit Act of 2010. The Act includes language that establishes predictive analytics technologies requirements for the Medicare fee-for-service program, directing the HHS Secretary to use predictive modeling and other analytics technologies to identify improper claims for reimbursement and prevent their payment. Last month, Secretary Sebelius announced that Northrop Grumman, together with National Government Services and Federal Network Systems, a Verizon company, had been selected to implement the predictive modeling and analytic technology requirements under the Small Business Jobs and Credit Act, beginning July 1.

NHCAA supports efforts among its members, both public and private, to shift greater attention and resources to predictive modeling, real-time analytics and other data intensive tools that will help detect fraud sooner and prevent its manifestation. We are particularly anxious to learn about the results of the predictive modeling project for Medicare fee-for-service now underway at HHS. Clearly one of Medicare's strengths in terms of fraud detection is the enormous amount of data the program generates and collects. Applying predictive modeling to that data could yield very powerful, game-changing results.

[8] These statistics are for the period of May 7, 2007 through September 30, 2010 as reported in the HCFAC Report for Fiscal Year 2010, http://oig.hhs.gov/publications/docs/hcfac/hcfacreport2010.pdf.

NHCAA
National Health Care Anti-Fraud Association

III. Investment in innovative health care fraud prevention, detection and investigation tools and programs is vital and should be encouraged.

There is no doubt that good work has been done in the fight against health care fraud. When it was established under 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."[9] Now, 14 years later, the documented success of the HCFAC affirms the wisdom of making that investment. Published in January 2011, the HCFAC report for Fiscal Year 2010 shows a return on investment (ROI) of $4.90 for every $1 spent since the program began. The three-year average ROI for Fiscal Years 2008-2010 is considerable at $6.80 to $1. According to the report, the HCFAC account has returned more than $18 billion to the Medicare Trust Fund since the program's inception. Similar to the HCFAC program findings, NHCAA's private-sector members consistently yield solid returns for their anti-fraud investments. It should be noted that, given the wide range in terms of size and scope of business of NHCAA's private insurer members, the ROI for anti-fraud activities varies from company to company.

More recent programmatic anti-fraud initiatives—including the HEAT program, the Medicare Strike Forces, as well as National and Regional Health Care Fraud Prevention Summits co-hosted by Secretary Sebelius and Attorney General Holder—have also demonstrated success and promise, employing collaborative approaches to prevent and identify health care fraud, and educating providers and beneficiaries about the problem of fraud. Moreover, the numerous anti-fraud tools enabled by the Affordable Care Act (ACA) are very good news for patients and taxpayers alike. For instance, the new screening requirements for providers participating in Medicare, Medicaid and the Children's Health Insurance Program (CHIP) are a big step in the direction of preventing fraud before it occurs by helping to deny access to these programs by

[9] See http://oig.hhs.gov/publications/docs/hcfac/hcfacreport2010.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 2010, page 3.

potential fraudsters. Based on the potential risk of fraud by categories of provider, the three levels of provider screening spelled out in the final rule will serve to protect our nation's health care investment.

The ACA also authorizes the Secretary to impose a temporary moratorium (6 months) on the enrollment of new providers of services and suppliers under Medicare, Medicaid and CHIP when necessary to prevent or combat fraud, waste or abuse. Notably, the final rule allows for moratoria in cases where CMS identifies a particular provider or supplier type and/or a particular geographic area as having a significant potential for fraud, waste or abuse. This is particularly important because health care fraud often manifests much like a fad would—it surfaces in one place or among one group, takes hold and proliferates. It is important to be able to suppress it when and where it appears in order to limit its reach.

Additionally, the ACA creates the ability of the Secretary to suspend payments to a specific provider "pending an investigation of a credible allegation of fraud." Several changes were also made to the Medicaid Integrity Program, including new provisions regarding exclusions from the Medicaid program. For instance, a provider's participation will be terminated under Medicaid if it has been terminated under Medicare or another state plan.

Among the many new anti-fraud provisions included as part of the ACA, additional funding for anti-fraud efforts was a noteworthy inclusion. The ACA allows for an additional $350 million to be appropriated to the fraud fighting cause between 2011 and 2020. NHCAA is confident that Congress and the public will be pleased with the results of this appropriation, as there is proven value in making anti-fraud investments.

The President's proposed budget for Fiscal Year 2012 is further acknowledgment that anti-fraud resources are sound investments. The budget proposes a $270 million increase for discretionary funding for Health Care Fraud & Abuse Control, and we applaud this commitment. The proposed increase is needed to fund the expansion of the strike forces and to advance the goal of shifting from the "pay and chase" fraud fighting concept to one that employs technology to

prevent and detect fraud prior to claims being paid. The return on investment for anti-fraud initiatives is significant, and therefore the increase in funding for these initiatives would be consistent with Congress' focus on reducing government spending.

These recent federal anti-fraud programs and initiatives, along with the substantial increase of funding and new anti-fraud tools enabled by the ACA, are very positive steps, particularly for government health programs. However, we question the regulatory decision to categorize anti-fraud activities undertaken by private insurers as simple "cost containment" in the medical loss ratio (MLR) interim final rules issued earlier this year. We believe this decision runs counter to the direction taken by the ACA. Consistent with the necessary priority given to anti-fraud efforts in the federal health care programs, private health plans should be given every incentive to invest in the technology and resources necessary to fight fraud and protect patients—particularly when the need to shift away from the "pay and chase" model is now. NHCAA is concerned that accounting for anti-fraud investments as "administrative" without acknowledging the quality-affirming aspects of this work will serve as a disincentive to private insurers to invest in fraud prevention. And we know that the nature of health care fraud demands constant reevaluation of methods and means and continual investment to stay ahead of the curve.

Public awareness and participation in the fight against health care fraud is also crucial to its success. We are encouraged to note that Senate Bill 1251 would change the beneficiary incentive program established under HIPAA to allow for monetary rewards to be paid prior to the full recovery of an overpayment. It also instructs the Secretary to use the Senior Medicare Patrols (SMPs) to conduct a "public awareness and education campaign" to encourage more participation in the incentive program. In 2010, NHCAA was proud to name the Senior Medicare Patrol program as the recipient of our Excellence in Public Awareness Award. This award is bestowed annually upon an organization or individuals who have done the most in the past year to raise public awareness about the problem of fraud in our nation's health care system. The SMP program is tireless in its commitment to fighting fraud in the Medicare system and would be an excellent partner for a campaign to promote the beneficiary incentive program.

Conclusion

Health care fraud costs taxpayers billions of dollars every year and often harms patients. Fighting it requires focused attention and a commitment to innovative solutions. NHCAA believes that a comprehensive approach to fighting fraud must include all payers, public and private. Additionally, multiple tools and methods must be applied. The anti-fraud efforts of organizations—private insurers and public payers alike—need to be flexible and multifaceted.

The schemes devised by perpetrators of health care fraud take many forms, and these perpetrators are opportunistic. Consequently, we must stay vigilant and work to anticipate and identify the risks, and develop strategies to meet these risks. Right now, harnessing the enormous quantities of data produced by our health care system in order to identify and predict fraud holds great promise. As Secretary Sebelius stated during the June Fraud Prevention Summit in Philadelphia, "We know that in order to stop health care fraud we also have to develop new methods and technologies to stay ahead of criminals and identify their patterns of behavior early." NHCAA encourages continued investment in exploring and implementing data consolidation and data analytical techniques.

NHCAA is encouraged by the renewed federal emphasis given to fighting health care fraud. This hearing is an excellent example, as are the statutes, regulations and policies from the past several years that have enabled greater fraud fighting success. NHCAA knows continued investment and innovation are critical, and as greater attention is given to eradicating fraud within our government health care programs, we urge decision makers to also recognize and encourage the important role that private insurers play in helping to minimize the fraud in our nation's health care system.

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

Questions for the Record
Dr. Peter Budetti, Deputy Administrator and Director for Program Integrity
Centers for Medicare and Medicaid Services

Senate Committee on Homeland Security & Government Affairs
Subcommittee on Federal Financial Management, Government Information, Federal Services and International Security
"Harnessing Technology and Innovation to Cut Waste and Curb Fraud in Federal Health Programs"
July 12, 2011

The Honorable Tom Carper

1. The Fraud Detection System – the combined Integrated Data Repository and One P.I. - is an important new tool to examine Medicare and Medicaid payments in order to detect fraud. However, the GAO has clearly shown that the system is not fully deployed. Also, the GAO reported that there are no clear plans, nor projected dates with specific milestones, to either train more people, or to integrate critical data sets, including the Medicaid data. And despite being part of the original design, there are no solid plans to give access to Medicaid state offices. Dr. Budetti, what is your planned schedule to fully implement and deploy the new Fraud Detection System?

More specifically, what are the CMS plans and schedules milestones for incorporating additional Medicare data into the IDR, including the shared system data and Medicaid data? Please include the target dates for full integration of the shared system data and Medicaid data.

Answer: The combined Integrated Data Repository (IDR) and One Program Integrity (PI) tool is one of the many tools used to detect fraud. CMS also began using predictive analytic technology on all nationwide Medicare fee-for-service (FFS) claims on a prepayment basis on June 30, 2011, as required by the Small Business Jobs Act of 2010. These two systems complement each other, as the work done in the IDR, specifically the testing and development of new predictive models, will be integrated into the Fraud Prevention System.

The IDR is a data warehouse that will integrate Medicare and Medicaid data into a single source for users across the agency. One PI is the analytic tool used to manipulate the data. It provides a multi-centric view of the data encompassing more than just claims data, but also beneficiary, plan and clinical perspectives (e.g. quality data).

The Fraud Prevention System is a predictive analytic tool that is being applied to all FFS claims before claims are paid. This allows us the ability to flag suspect claims using predictive analytics, through risk algorithms, and conduct prepayment review. The system continuously incorporates new data into existing risk profiles, and automatically sets workload priorities for our contractors.

We chose to incorporate Medicare Part A and B data into the IDR first because, due to the size and scope of the Medicare fee-for-service program, it poses the greatest potential risk to the Trust Funds in terms of potential dollars lost. To date, the IDR contains:
Part A paid claims data for the past 7 years
Part B paid claims (including Durable Medical Equipment (DME) data) data for the past 7 years
Part D paid claims data (Prescription Drug Event data) for the past 7 years

CMS plans to incorporate the remaining shared systems data (the pre-pay portion) in the IDR by March 2012. Although CMS had initially developed an aggressive timetable, we have had to revise the plan to reflect the changing resources and capacity of the agency. In addition, we have needed time to address the variations in the types of formats of Medicaid data stored in disparate State Medicaid systems, and time to work through complex data development issues associated with the multitude of different shared systems within CMS.

CMS also plans to incorporate Medicaid data for all 50 states by the end of FY2014. Incorporating State Medicaid data into the IDR is a priority for us and we are working diligently to meet the 2014 goal. We are aware that States have competing priorities in a tightened fiscal environment and we are working closely with them to help streamline data requests under the agency's Medicaid and CHIP Business Information and Solutions (MACBIS) data initiative.

2. What are the plans and schedule milestones for training all program integrity analysts to use One PI/Integrated Data Repository? What are the plans and schedule milestones for training and providing access for federal law enforcement staff at the Department of Justice and HHS Office of Inspector General?

Answer: CMS plans to train all appropriate Zone Program Integrity Contractor (ZPIC) staff by December 2011. CMS also plans to continue to train law enforcement as needed. There is no established cap for the number CMS will train, however, we have doubled the number of training courses available this year as well as redesigned our training course so that it is more meaningful to IDR users. After we began training users for the first time, we received feedback that additional instruction was needed. We significantly restructured the training courses to give users more hands-on instruction with the data systems tool and provide one-on-one data training led by "data coaches." While the redesign delayed CMS' plans to train the intended number of users, we are confident the training program now has the capability to provide IDR users with the skills they need to detect fraud.

3. What are the plans and schedule milestones for providing One PI/Integrated Data Repository training and access to Medicaid state offices, as well as state program integrity offices and law enforcement offices?

Answer: CMS is collaborating closely with States to improve data systems to address the data needs of Federal and State Medicaid partners. CMS is working actively with 10 States to "test drive' a new data submission methodology and CMS anticipates this pilot will improve data quality and timeliness, as well as reduce both data and process redundancies. We believe that these improvements will be important for program integrity analysis in the future.

The Honorable Ron Johnson

1. You've mentioned a lot of tools to catch more people defrauding federal health programs. Apart from improper payments, such as errors, and talking just about actual fraud:

- **a. What are the fraud rates in Medicare and Medicaid now?**
- **b. What sort of rate do you expect to be able to hit with these new tools?**
- **c. Name a specific number, please.**
- **d. What's your timetable for reaching that target fraud rate?**

Answer:
a. We do not have an exact dollar amount about how much money is lost to fraud in our programs as there is yet no agreed upon method to estimate fraud in the Medicare and Medicaid programs. However, CMS is collaborating with the HHS Assistant Secretary for Planning and Evaluation (ASPE) to develop a pilot measurement of the amount of probable fraud for certain services in the Medicare program. We expect significant progress will be made to develop fraud rates for Home Health and Durable Medical Equipment over the next year.

b. After the pilot year, we expect to establish a baseline of fraud for Home Health and DME to measure future success. We are also committed to the President's goal of reducing the Medicare FFS improper payment rate by 50 percent by 2012. While the improper payment rate does not measure the fraud rate in Medicare, we do believe our antifraud activities will contribute to other agency efforts to reduce the improper payment rate.

c. As stated above, in the absence of the baseline probable fraud measurement, we are committed to reducing the improper payment rate in Medicare FFS to 6.2 percent in 2012.

YEAR	TARGET IMPROPER PAYMENT RATE
2011	8.5%
2012	6.2%

d. We are unable to establish a target fraud rate without a baseline probable fraud measurement. CMS remains committed to rooting out fraud in the absence of such a rate, and have used many tools to do so to date. The Fraud Prevention System has been screening all FFS claims since June 30, 2011; providers designated moderate or high risk have been undergoing site visits upon enrollment or revalidation and CMS has had the authority to impose payment suspensions since March 25, 2011. CMS is continuing to implement the ACA and make additional investments in technology. For example, CMS anticipates implementing automated enrollment screening in January 2012 that will continuously monitor enrollment requirements and reduce contractor workload.

2. You testified that CMS is committed to developing the means of measuring the reduction of fraud.
- **a. What sorts of measures are you developing?**
- **b. When do you expect to put them in place?**
- **c. What specific quantitative measures will you be gauging?**

Answer:
a. As stated above, CMS is collaborating with the Assistant Secretary for Planning and Evaluation (ASPE) to develop a pilot measurement of the amount of probable fraud for certain services in the Medicare program. The measurement design is currently underway, and the pilot will be applied to two high-risk service categories – DME and Home Health. The size of the pilot will result in a national rate for these two categories. We intend on using the lessons learned from the pilot to expand the measurement methodology to other service categories. We are also considering approaches to measuring cost avoidance, which would reflect successful fraud prevention but is more difficult to quantify than recoveries.

b. CMS is in the process of developing the measure, and is anticipating the implementation of the pilot in early 2012, and a calculated baseline rate to be available from the pilot next year.

c. One of the main challenges with measuring fraud or probable fraud is that it is not a simple quantitative measure. While this pilot will rely on data analysis to provide context to a claim, many of the pieces will come through qualitative information, such as provider site visits and interviews. We anticipate engaging a panel of experts to review the data for each claim. We anticipate that this will result in a semi-quantitative rate of probable fraud.

3. You testified that you'll seek better measures of how much fraudulent payment you stop. That will be a useful number indeed.

- **a. Will you be able to measure whether you're stopping an increasing share of all fraud committed against Medicare and Medicaid?**
- **b. What are you doing to develop such measures?**

Answer:

a. We are looking forward to seeing what type of information this pilot measurement will provide us. As I stated in my testimony, we are committed to preventing fraud and anticipate that the baseline and future measurements can capture the success of our many antifraud initiatives. Moreover, we are also considering approaches to measuring cost avoidance, which would reflect successful fraud prevention but is more difficult to quantify than recoveries.

b. As stated above, we are developing the methodology for a probable fraud rate, and expect a pilot measurement for home health and DME to be available in approximately one year. We will incorporate lessons learned from the pilot to refine these measures and to develop measures for other service categories.

Subcommittee on Federal Financial Management, Government Information, Federal Services and International Security
"Harnessing Technology and Innovation to Cut Waste and Curb Fraud in Federal Health Programs"

July 12, 2011

For Lewis Morris, Chief Counsel to the Inspector General, U.S. Department of Health and Human Services

1) The Affordable Care Act is due to expand Medicaid by about 20 to 25 million patients. You told the panel that "with the expansion of the benefits . . . there will be a greater threat to the program."
    a. Can you quantify that increase, in proportional or dollar terms?
    b. Will the expansion increase the program's fraud rate?

    Although beneficial to Medicaid recipients, the introduction of new benefits and services also introduces new opportunities for abuse by those who prey on the program. While there is no precise measure of the magnitude of health care fraud, we know that it is a serious problem that demands an aggressive response. As exemplified by the Medicare Fraud Strike Forces, sophisticated data analysis, combined with field intelligence and traditional law enforcement techniques, have enabled us to more quickly identify fraud schemes and trends. The data-driven approach of the Strike Forces pinpoints fraud hot spots through the identification of suspicious billing patterns and targets criminal behavior as it occurs. The Strike Force model has proven highly successful and has accelerated the Government's response to criminal fraud, decreasing by roughly half the average time from an investigation's start to the case's prosecution. Since their inception in 2007, Strike Force teams have charged over 1,000 individuals with seeking to defraud Medicare of more than $2.4 billion.

2) One of the tools in the Affordable Care Act is the power for the secretary to suspend payments to a specific provider "pending an investigation of a credible allegation of fraud." You testified that there have been 53 such suspensions, stopping the payment of more than $8 million in benefits.
    a. Of those suspensions, how many have been conclusively demonstrated to have been fraud?
    b. In what share of those cases have the beneficiaries or providers involved been cleared of suspicion and the payments gone forward?
    c. Since these suspensions happen upon "credible allegation," can we suppose that as the mechanism is used more frequently, some honest providers might be cut off from time to time?

d. Does the government have a mechanism to make whole any providers whose payments were cut off but who were later cleared of suspicion?

Under the new payment suspension authority in the Affordable Care Act (ACA), the Secretary can suspend payments to a provider or supplier pending an investigation of a credible allegation of fraud against the provider or supplier. There are good cause exceptions not to suspend or not to continue to suspend payments. The Secretary is required to consult with the OIG in determining whether there is a credible allegation of fraud. ACA also amends the relevant Medicaid provisions with respect to suspending Medicaid payments.

OIG works closely with the Centers for Medicare & Medicaid Services (CMS) to suspend payments in cases where we have credible evidence of fraud. For example, during a July 2010 Strike Force operation, OIG worked with CMS to initiate payment suspensions and pre-pay edits on 18 providers and suppliers targeted by the investigation. The prompt action taken by OIG and CMS stopped the potential loss of over $1.3 million in claims submitted by the defendants. During the February 2011 Strike Force operations, OIG and CMS worked to impose payment suspensions that immediately prevented a loss of over a quarter million dollars in claims submitted by Strike Force targets.

Payment suspension is an effective fraud fighting tool, used judiciously and selectively, to target high risk fraud, with minimal likelihood of impacting innocent providers. It is a short-term solution, after which payment is restored if allegations are not meritorious. All of the 53 suspensions referenced in my testimony are currently active and the cases are still ongoing investigations. Of the 53 suspended providers, 34 have been either arrested, charged, indicted, or have pled guilty. None of the cases have been adjudicated to date. None of the 53 providers have been cleared or the payments gone forward.

During the suspension period, CMS contractors will request that the provider submit medical records relevant to any suspect claims being examined by CMS. A Medicare contractor (typically a Zone Program Integrity Contractor (ZPIC) or Program Safeguard Contractor (PSC)) will then analyze these medical records in order to determine the amount of any improper payments made to the provider, including overpayments. Once the overpayment has been calculated, a provider's Medicare Administrative Contractor will issue a demand letter to the provider requesting a refund of the overpayment amount. In some instances, once CMS has ascertained the nature and extent of any overpayment, the suspension action will be lifted.

Health care providers may continue to submit claims during a suspension period, but payment action for these claims will not be taken until the ZPIC / PSC can determine the nature and amount of any overpayment that may be owed. Any claims found to qualify for coverage and payment are usually used to offset the amount of the overpayment determined by the ZPIC / PSC. Excess funds are then distributed to the provider.

3) If these new tools will catch more fraudsters, that should mean less fraud.
   a. Can we expect a decline in fraud because of a deterrent effect?
   b. Do you know whether past anti-fraud efforts have had a deterrent effect?
   c. Which techniques offer the best deterrent effect?
   d. How do you measure that?

OIG measures outcomes of investigations in terms of expected and actual returns and criminal, civil, and administrative actions. Although it is much more difficult to measure, we believe that our oversight and enforcement work has a strong "sentinel effect" in deterring fraud. For example, during the first year of our Strike Force operations in Miami, which cracked down on Medicare durable medical equipment (DME) fraud, submissions of DME claims decreased by 63 percent, representing a decrease of $1.75 billion, compared to the previous year. Other non-measurable but important preventive outcomes include fraud averted, such as by preventing bad actors from obtaining Medicare billing privileges or preventing fraudulent claims from being paid through pre-payment review.

Though the sentinel effect is difficult to quantify, anecdotal evidence shows industry is embracing compliance programs. From compliance efforts, we would expect a decline in certain types of fraud due to increased awareness, training, avoidance, and reporting. OIG has a robust self-disclosure program, which rewards providers that effectively use compliance programs to identify and report evidence of fraud. Since 1998 the self-disclosure program has resulted over $266 million dollars in expected recoveries to the Medicare trust funds. We believe the success of this program demonstrates the value of compliance efforts.

Compliance, along with prevention and enforcement, is a key aspect of program integrity. A key part of OIG's health care integrity strategy is to educate and assist well-intentioned providers in fully complying with Medicare laws and regulations. We have developed a number of tools that include compliance program guidance, including our Health Care Fraud Prevention and Enforcement Action Team (HEAT) provider compliance training (http://oig.hhs.gov/compliance/provider-compliance-training/index.asp) and *A Roadmap for New Physicians* (http://oig.hhs.gov/compliance/physician-education/index.asp). The impetus to devote resources to compliance often leads to improved attention to, and compliance with, Medicare laws governing reimbursement and saves the Government money and resources in combating fraud.

Moreover, the ACA contains numerous new tools and resources that will assist OIG's anti-fraud efforts. In addition to providing critical Health Care Fraud and Abuse Control Program (HCFAC) funding, ACA also enhances the Federal sentencing guidelines to provide stiffer penalties for health care offenses, changes the anti-kickback statute to strengthen the Government's ability to prosecute those who pay illegal kickbacks, and enhances authority to suspend payments pending the investigation of credible allegations of fraud, which will help ensure that the government can more effectively stop perpetrators from absconding with ill-gotten program funds. The foregoing measures provide powerful deterrence to criminals who are considering a career in health care fraud.

Ultimately, an effective fraud-fighting strategy must include prevention, compliance, and enforcement efforts. The goal is to prevent fraud by keeping unscrupulous providers out of Medicare and helping well-intended providers avoid fraud risks. However, these measures won't prevent fraud completely. Strong enforcement measures are also essential to redress fraud and to help deter other criminals from targeting Medicare.

4) There's a lot of good language in the FAST Act about sharing information between agencies, and you mentioned the working groups that sometimes share information with private insurers. Mr. Saccoccio made a point of testifying that we must include private payers.
   a. Are federal agencies not doing this consistently?
   b. Is there a way to make that kind of cooperation more widespread and permanent?
   c. You mentioned you want the "spirit of the law" to be embraced. Is that something legislation can help accomplish?

OIG is always looking for opportunities to more effectively utilize our resources, a key aspect of which is leveraging public and private partnerships. One key impediment to information sharing between the public and private sector is a lack of understanding of what is permissible under the law. As mentioned in my testimony, OIG is reviewing the results of a survey of our law enforcement partners to identify current practices and impediments to information sharing with the private sector.

However, there are many encouraging efforts underway. A key part of OIG's health care integrity strategy is to educate and assist well-intentioned providers in fully complying with Medicare laws and regulations. We have developed a number of tools that include compliance program guidance, including our HEAT provider compliance training (http://oig.hhs.gov/compliance/provider-compliance-training/index.asp) and *A Roadmap for New Physicians* (http://oig.hhs.gov/compliance/physician-education/index.asp). The impetus to devote resources to compliance often leads to improved attention to, and compliance with, Medicare laws governing reimbursement and saves the Government money and resources in combating fraud.

OIG also participates in outreach calls sponsored by CMS which are open to the provider community. The purpose of these calls is to educate providers and suppliers on specific vulnerabilities identified in our reports. During the calls OIG representatives, CMS Contractor Medical Directors, and CMS personnel address topics related to Medicare policy, billing instructions and medical review guidance related to reducing improper payments.

My written statement also describes the recent HEAT fraud summits, as well as Health Care Fraud Working Groups, which have brought together Government agencies and private sector insurers united in the common goal of combating health care fraud.

Regarding legislation that might facilitate information sharing, OIG has provided the Committee with technical assistance on amendment of 1128E of the Social Security Act to create a national health care fraud and patient abuse data collection program. This program would create a central repository of final adverse action data on individuals and

entities, including health care providers, practitioners, suppliers, and direct patient access employees, and maintain this information in a database accessible to the public, with certain exceptions. We would be happy to provide further technical assistance on request.

5) All of you alluded at one point or another in your testimony about problems stemming from your work with other organizations. Mr. Morris said that "contractors often disappoint us." Mr. Willemssen talked about holding states' "feet to the fire" about how they format their data. Dr. Budetti brought up the failings of contractors, states and providers. You have my support in overcoming these challenges. But leaving those aside for a moment:
    a. Can you each say what you see as the weakest part of the federal government's own performance in preventing fraud against Medicare and Medicaid?
    b. What did the federal government not do right?
    c. What specific part of federal performance and systems are ripest for improvement?

There are many opportunities for the Federal government to improve. In my testimony, I spoke about persistent vulnerabilities in CMS's oversight of the program integrity contractors who play a crucial role in safeguarding the Medicare and Medicaid programs. For well over a decade, OIG has found that contractors performed inconsistently – but CMS could not explain why. We found that CMS's evaluations of contractors did not include sufficient information, and were not timely enough to be used in assessing contractors' performance prior to contract renewals. We also found that CMS sometimes failed to give contractors the data access needed to accomplish their objectives. Furthermore, even when CMS explicitly recognized the importance of conducting proactive data analysis to uncover fraud and abuse, that new focus was not successfully implemented at the contractor level; we found that program integrity contractors produced minimal results in this key area. We are hopeful that CMS's new predictive modeling contracts will result in the increased use of technology and analytics to reduce Medicare payments to fraudulent providers. Although these new information technologies hold promise, even the best fraud prevention techniques will be of no value if not effectively implemented and appropriately overseen. OIG work has revealed consistent weaknesses in Federal oversight that must be remedied in order for future program integrity contracting efforts to succeed.

An equally important factor in safeguarding Medicare is ensuring that only legitimate providers are allowed into the program. Unfortunately, provider enrollment has historically been a serious vulnerability. Past OIG work has demonstrated that all too often, sham providers and suppliers are able to obtain Medicare billing numbers and bill for millions of dollars in fraudulent claims. In the wake of new ACA requirements, CMS has made changes to provider enrollment screening and oversight that show promise. However, given the severity of this problem in the past, and the critical role of provider enrollment safeguards in protecting Federal health care programs, this area should continue to be a focus for improvement.

Within the Medicaid program, the lack of timely, accurate data poses a serious barrier to program integrity efforts. Currently, two primary data sources are available: the

Medicaid Statistical Information System (MSIS) and the Medicaid Management Information Systems (MMIS). Neither database allows for the type of robust data analysis that oversight entities should ideally conduct. For example, MMIS does not include all variables necessary to make key determinations – for example, information about who is enrolled and receiving Medicaid services through a waiver is necessary to determine who is entitled to certain services. Additionally, MMIS includes service-specific claims only for services provided on a fee-for-service basis. However, well over half of beneficiaries receive all or some services through managed care. MSIS is intended to include both fee-for-service and managed care data, but OIG has found that in practice, not all managed care data is reported. CMS's Integrated Data Repository, operational since September 2006, was intended to include both Medicare and Medicaid data; however, GAO recently reported that Medicaid data has not been integrated into the system, and CMS has not finalized plans or developed reliable schedules for efforts to do so. Without complete, timely, accurate data, the types of innovative data analytics being implemented for Medicare oversight are not options for Medicaid oversight.

Post-Hearing Questions for the Record

Submitted to the Honorable Lewis Morris

From Senator Mark L. Pryor

"Harnessing Technology and Innovation to Cut Waste and Curb Fraud in Federal Health Programs"

July 12, 2011

1. In your testimony, you discussed ways that your office is working with the private sector to address fraud. You specifically mentioned working on a health care fraud summit. What other types of fraud awareness and prevention events or initiatives will your office collaborate on with members of the private sector?

There are many encouraging efforts underway. A key part of OIG's health care integrity strategy is to educate and assist well-intentioned providers in fully complying with Medicare laws and regulations. We have developed a number of tools that include compliance program guidance, including our Health Care Fraud Prevention and Enforcement Action Team (HEAT) provider compliance training (http://oig.hhs.gov/compliance/provider-compliance-training/index.asp) and *A Roadmap for New Physicians* (http://oig.hhs.gov/compliance/physician-education/index.asp). The impetus to devote resources to compliance often leads to improved attention to, and compliance with, Medicare laws governing reimbursement and saves the Government money and resources in combating fraud.

OIG also participates in outreach calls sponsored by the Centers for Medicare & Medicaid Services (CMS) which are open to the provider community. The purpose of these calls is to educate providers and suppliers on specific vulnerabilities identified in our reports. During the calls OIG representatives, CMS Contractor Medical Directors, and CMS personnel address topics related to Medicare policy, billing instructions and medical review guidance related to reducing improper payments.

We have also have produced beneficiary education materials relating to medical identity theft (http://oig.hhs.gov/fraud/medical-id-theft/index.asp) and work with the Senior Medicare Patrol units to educate beneficiaries about how to prevent, identify, and report fraud, waste, and abuse.

My written statement more fully describes the recent HEAT fraud summits, as well as Health Care Fraud Working Groups, which have brought together Government agencies and private sector insurers united in the common goal of combating health care fraud.

2. You pointed out in your testimony that as we become more adept and savvy at finding fraud, people who want to cheat the system simultaneously become more adept and savvy. How do we stay ahead of the curve? Are there resources in place to identify weaknesses before they are exploited?

Although the majority of health care providers are honest and well-intentioned, a minority of providers who are intent on abusing the system cost taxpayers billions of dollars. Those intent on breaking the law are becoming more sophisticated, and the schemes are more difficult to detect. Some fraud schemes are viral, i.e., schemes are replicated rapidly within communities. Health care fraud also migrates – as law enforcement cracks down on a particular scheme, the criminals may redesign the scheme (e.g., suppliers fraudulently billing for durable medical equipment (DME) have shifted to fraudulent billing for home health services) or relocate to a new geographic area. The Medicare program also is increasingly infiltrated by violent and organized criminal networks.

Collaboration and innovation are essential in the fight against health care fraud. On May 20, 2009, the HHS Secretary and the Attorney General announced the creation of HEAT. This initiative marshals significant resources across the Government to prevent health care waste, fraud, and abuse; crack down on those who commit fraud; and enhance existing partnerships between HHS and the Department of Justice (DOJ).

Medicare Fraud Strike Forces are an essential component of HEAT and have achieved impressive enforcement results. Strike Forces are designed to identify and investigate fraud, and prosecute the perpetrators quickly. Strike Force teams are composed of dedicated prosecutors from DOJ and U.S. Attorneys Offices and Special Agents from OIG; the Federal Bureau of Investigation (FBI); and, in some cases, State and local law enforcement agencies. These "on the ground" enforcement teams are supported by data analysts and program experts. This coordination and collaboration have accelerated the Government's response to criminal fraud, decreasing by roughly half the average time from the start of an investigation to its prosecution. The data-driven

approach of the Strike Forces pinpoints fraud hot spots through the identification of suspicious billing patterns and targets criminal behavior as it occurs. The Strike Force model has proven highly successful and has accelerated the Government's response to criminal fraud, decreasing by roughly half the average time from an investigation's start to the case's prosecution. Since their inception in 2007, Strike Force teams have charged over 1,000 individuals with seeking to defraud Medicare of more than $2.4 billion.

OIG's new hospital compliance initiative illustrates how technology is enhancing our ability to identify suspect claims and non-compliant billing practices. Payments for inpatient and outpatient hospital services account for roughly 30 percent of the $515 billion spent on Medicare. In the past, OIG's hospital audits typically focused on a specific area of risk (e.g., unbundling of services, inpatient same-day discharges and readmissions, and credits for medical devices), and we audited claims exclusively related to that issue. In part, we had narrowly focused our audits due to limits on our capacity to store and match data. As a consequence of increased data storage, computer matching, and data analytic capabilities, we are now more quickly and efficiently analyzing a vast array of hospital data to simultaneously identify multiple compliance risks. Two years ago, the data analytics would have taken weeks or months to execute. Now, it takes approximately 20 minutes to run the computer program for each hospital.

And as noted in the response to question 1 above, we are partnering with public and private sector entities to educate providers and beneficiaries about how to prevent, identify, and report fraud, waste, and abuse.

Regarding additional resources, the FY 2012 President's Budget request includes $581 million in Health Care Fraud and Abuse Control Program (HCFAC) discretionary funding for the combined efforts of OIG, CMS, and DOJ to provide oversight of Medicare and Medicaid. Moreover, the Budget Control Act of 2011 includes comparable adjustments to the discretionary spending limits set forth in the Act for these combined efforts through 2021.

The increased funding would support important fraud-fighting efforts, including enhanced data analysis and collaborative approaches for detecting suspected fraud more effectively and "boots on the ground" for our vital oversight and enforcement efforts.

GAO
Accountability • Integrity • Reliability
United States Government Accountability Office
Washington, DC 20548

September 23, 2011

The Honorable Ron Johnson
Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security
Committee on Homeland Security and Governmental Affairs
United States Senate

Dear Mr. Johnson:

This letter responds to your recent questions related to our July 12, 2011, testimony on the Centers for Medicare and Medicaid Services' (CMS) use of information technology to help improve the detection of fraud, waste, and abuse in the Medicare and Medicaid programs.[1] At that hearing, we discussed CMS's progress in developing, implementing, and achieving its goals and objectives for its Integrated Data Repository and One Program Integrity systems to detect fraud, waste, and abuse. Your questions, along with our responses, follow.

Question 1: *Mr. Morris testified that cybersecurity is "a great concern." Since a substantial number of the fraud schemes that HEAT teams are catching seem to involve some form of stolen or faked identify, please assess for us:*

a. PPACA's new anti-fraud measures notwithstanding, the expansion of federal health programs will present new opportunities for determined fraudsters?

We have not conducted studies that specifically addressed fraud associated with the expansion of federal health programs; however, the results of our work related to the need to protect information systems in other federal programs suggest that the increase in the numbers of beneficiaries and providers in the Medicare and Medicaid programs as a result of expanded federal health programs could present new targets and opportunities for determined fraudsters. We testified in March 2011 that cyber-based threats to critical infrastructure and federal systems are evolving and growing.[2] In this regard, reports of security incidents from federal agencies are on the rise, increasing over 650 percent over the past 5 years. Moreover, personally identifiable information about U.S. citizens has been lost, stolen, or improperly disclosed, thereby potentially exposing those individuals to loss of privacy, identity theft, and financial crimes. Contributing to this situation is that federal systems

[1]GAO, *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).
[2]GAO, *Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure and Federal Information Systems*, GAO-11-463T (Washington, D.C.: Mar. 16, 2011).

continue to be afflicted by persistent information security control weaknesses. As part of our audit of the fiscal year 2010 federal financial statements, we determined that serious and widespread information security control deficiencies were a governmentwide material weakness.

Likewise, we reported in 2006 that CMS's information network had security weaknesses that placed financial and personally identifiable medical information transmitted on the network at increased risk of unauthorized disclosure.[3] We found that CMS relied extensively on a computerized network of systems that supported its mission-critical operations and transmitted and stored the sensitive information it collected. In particular, the agency relied on a contractor-owned and operated network to provide connectivity to its business partners. This network supported communication and data transmission between CMS business-related entities, including the CMS central office and data center, CMS regional offices, financial institutions, Medicare intermediaries and carriers, Medicare data centers, skilled nursing facilities, and home health agencies. The communication network transmitted Medicare claims data containing personally identifiable information such as name, sex, date of birth, Social Security number, and address. It also transmitted medical information, such as a patient's diagnosis, prescribed drug and drug dosage, type of treatment facility—which can include substance abuse facilities or psychiatric treatment centers—requested service, and the physician's name and identification number. While CMS agreed with the need for and took actions aimed at correcting deficiencies in its security policies and controls, expanded health programs and any resulting increases in the numbers of Medicare and Medicaid beneficiaries and providers could present additional targets and opportunities for those determined to carry out acts of fraud against these programs.

Question 2: *Mr. Morris alluded to fraudsters testing anti-fraud systems and adapting.*

a. Can we expect that some level of fraud is endemic to running a large, complex payment system?

While we have not studied the level of fraud specifically related to large, complex payment systems, as noted above, reported threats to federal information systems are evolving and growing. These threats could involve the use of such systems in the commission of fraudulent activities against government programs including those that process claims and pay benefits. GAO recently issued its updated high-risk list of government programs that have greater vulnerability to fraud, waste, and abuse.[4] Among these is CMS's Medicare program, which has been included on the list since 1990, in part because the program's size and complexity make it vulnerable to fraud, waste, and abuse. For example, we noted that Medicare had estimated improper payments of almost $48 billion, which did not represent all of the program's risk. In addition, the Medicaid program is on the high-risk list because of concerns about the adequacy of fiscal oversight, which is necessary to prevent inappropriate program spending.

[3]GAO, *Information Security: The Centers for Medicare & Medicaid Services Needs to Improve Controls over Key Communication Network,* GAO-06-750 (Washington, D.C.: Aug. 30, 2006).
[4]GAO, *High-Risk Series: An Update,* GAO-11-278 (Washington, D.C.: February 2011).

As public and private organizations increasingly rely on computer systems to transfer money and sensitive information, the security of these systems and data is essential to protecting against fraudulent activities. Conversely, ineffective information security controls can result in significant risks, including the loss of resources, such as federal payments and collections.

b. Could simplifying the payment structure of federal health programs to reduce the number of transactions reduce the opportunities for cybersecurity-based fraud?

We have not studied the impact that simplifying the payment structure of federal health programs would have on the opportunities for cybersecurity-based fraud. However, our 2006 study of CMS's implementation of information security controls described the expansive communication network which transmits payment information among many providers, payers, states, and contractors to support payments of Medicare claims. We indicated in our report that dramatic expansions in computer interconnectivity require proper safeguards to help ensure that systems are protected from individuals and groups intending to intrude and use their access to commit fraud and other malicious acts.

Question 3: *All of you alluded at one point or another in your testimony about problems stemming from your work with other organizations. Mr. Morris said that "contractors often disappoint us." Mr. Willemssen talked about holding states' "feet to the fire" about how they format their data. Dr. Budetti brought up the failings of contractors, states, and providers. You have my support in overcoming these challenges. But leaving those aside for a moment:*

a. Can you each say what you see as the weakest part of the federal government's own performance in preventing fraud against Medicare and Medicaid?

Our prior work has identified weaknesses in CMS's performance in preventing fraud against Medicare and Medicaid related to (1) the oversight of contractors and other non-federal entities involved in program administration, (2) provider enrollment standards and procedures, (3) prepayment review of claims, (4) postpayment review of claims, and (5) addressing identified program vulnerabilities.[5] Medicare is administered through contractors, plans, and drug sponsors. In this regard, contractors process and pay claims, enroll providers, and investigate potential Medicare fraud. Plans and drug sponsors also play a role in protecting the program from fraud. Medicaid is administered through a shared governance structure under CMS oversight, with more than 50 distinct state-based programs. Like Medicare, the state Medicaid programs rely on contractors to help manage payments and services. As such, states also play a critical role in implementing strategies to address fraud. Nonetheless, despite the key role that these non-federal entities play in

[5]GAO, *Medicare Fraud, Waste, and Abuse: Challenges and Strategies for Preventing Improper Payments*, GAO-10-844T (Washington, D.C.: June 15, 2010).

administering the Medicare and Medicaid programs, our work has identified ineffective oversight of their activities and, accordingly, we have noted the need for CMS to institute stronger procedures, standards, and controls to help prevent fraud in these important programs.

b. What did the federal government not do right?

In 2008, we found that CMS's oversight of prescription drug plan sponsors' compliance with requirements to establish programs for addressing potential fraud and abuse had been limited.[6] In particular, the drug plan sponsors had not included all of the required fraud and abuse compliance plan elements, and CMS had not conducted oversight to assess the compliance programs. To help improve oversight of this area, we recommended that CMS conduct timely audits of the sponsors' fraud and abuse programs. Subsequently, CMS began auditing the programs, and in 2010, conducted on-site compliance plan audits of 33 of 290 sponsors, which represented 11 percent of sponsors and covered 62 percent of enrolled beneficiaries.

Additionally, results of a series of reports beginning in 2005 indicated that CMS had not established effective provider screening procedures to help reduce the risk of enrolling providers intent on defrauding or abusing the program.[7] As a result, we recommended that CMS take steps to improve the provider enrollment process. However, even after some agency efforts to strengthen enrollment were made, we were still able to set up two fictitious medical equipment supply companies using undercover names and bank accounts and obtain approval to bill Medicare, despite having no clients or inventory.

Further, the agency had not required contractors to use automated prepayment edits and controls that could help prevent fraud in the Medicare program. In reporting on this matter in January 2007,[8] we recommended that CMS require its contractors to establish thresholds for unexplained increases in billing and use them to develop edits to identify potentially fraudulent billing transactions before paying claims. We also found that CMS had not required state Medicaid agencies to use some specific prepayment edits that have been used in the Medicare program to help identify fraudulent claims. Such controls would include, for example, edits to help determine whether providers meet federal and state requirements for enrolling in the Medicaid program.

Finally, although CMS's post-payment review efforts increased with the use of recovery audit contractors, we found that the agency was not using information from

---

[6]GAO, *Medicare Part D: CMS Oversight of Part D Sponsors' Fraud and Abuse Programs Has Been Limited, but CMS Plans Oversight Expansion,* GAO-10-481T (Washington, D.C.: Mar. 3, 2010).
[7]GAO, *Medicare: Improvements Needed to Address Improper Payments in Home Health,* GAO-09-185 (Washington, D.C.: Feb. 27, 2009); *Medicare: Covert Testing Exposes Weaknesses in the Durable Medical Equipment Supplier Screening Process,* GAO-08-955 (Washington, D.C.: July 3, 2008); and *Medicare: More Effective Screening and Stronger Enrollment Standards Needed for Medical Equipment Suppliers,* GAO-05-656 (Washington, D.C.: Sept. 22 2005).
[8]See GAO, *Medicare: Improvements Needed to Address Improper Payments for Medical Equipment and Suppliers,* GAO 07 59 (Washington, D.C.: Jan. 31, 2007).

these contractors about vulnerabilities to improper payments.[9] As a result, we recommended that the agency develop a robust process to establish corrective actions.

c. What specific part of federal performance and systems are ripest for improvement?

As the agency continues its efforts to develop and implement several significant information technology initiatives, program officials have opportunities to implement features and functionality intended to improve systems' performance in supporting fraud prevention activities. As noted during the hearing, our June 2011 report[10] identified deficiencies in certain areas of the management of two systems development projects which could benefit from improvements in planning processes. We described in our report and testimony[11] the status of the development and implementation of the Integrated Data Repository (IDR), a large central data store which provides program integrity analysts data related to claims that have been paid under the Medicare Parts A and B programs, as well as the prescription drug program. As a result of our study of IDR, we found that CMS had not yet developed features and functionalities to incorporate and allow the analysis of prepayment claims and Medicaid data. Inclusion of these features and functionalities could help improve the performance of the analytical tools that access data from IDR and, thus, of the analysts who use the tools to help detect potentially fraudulent claims. While this system is designed to help identify and prevent improper payments, the information provided by the system could be used by CMS to help prevent fraud from occurring. For example, any cases of potential fraud that would be flagged as a result of using the system, and then confirmed by investigative activities, could indicate patterns of behavior or identify individual providers to target in fraud prevention activities.

CMS has another opportunity to enhance its fraud prevention capabilities through the ongoing implementation of new information technology systems. In July 2011, the agency reported that it had implemented a predictive analytic system that is to be used to review claims before they are paid, so that the claims can be analyzed to identify patterns of billing that could be indicative of fraud. According to CMS, the use of the system is also intended to help prevent fraudulent activity from occurring. We are initiating a review of this effort to identify how the system is being implemented into CMS's information technology infrastructure and determine what actions CMS and its contractors are taking when potentially fraudulent billing is identified. As it continues the development and implementation of the system, it is important that the agency considers and addresses recommendations we made regarding IDR to ensure that system features and functionalities are delivered on schedule and that they meet the needs of CMS staff and contractors who work toward preventing fraud.

---

[9]GAO, *Medicare Recovery Audit Contracting: Weaknesses Remain in Addressing Vulnerabilities to Improper Payments, Although Improvements Made to Contractor Oversight,* GAO-10-143 (Washington, D.C.: Mar. 31, 2010).
[10]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).
[11]GAO-11-822T

Finally, CMS has opportunities to further improve its performance toward preventing fraud in Medicare and Medicaid in as it implements new requirements of the Patient Protection and Affordable Care Act (PPACA) and other recent legislation and administrative directives.[12,13] Among other things, the act includes additional requirements related to the strengthening of provider enrollment and inclusion of specific prepayment edits. For example, PPACA required states to implement screening practices to determine whether providers meet federal and state requirements for enrolling in the Medicaid program. The act also required states to incorporate into their Medicaid Management Information System compatible National Correct Coding Initiative methodologies in order to promote correct coding on claims.[14] In addition to the work we are beginning on the predictive analytics system, we have begun to assess CMS's efforts to address PPACA requirements to strengthen the standards and procedures for Medicare provider enrollment. We are also examining the effectiveness of different types of prepayment edits in Medicare and of CMS's oversight of its contractors in implementing those edits.

To respond to these questions, we relied on previously reported information. The work supporting these reports was conducted in accordance with generally accepted government auditing standards and guidelines established by the President's Council for Integrity and Efficiency. The auditing 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 provides a reasonable basis for our findings and conclusions based on our audit objectives.

Should you or your staff have any questions about matters discussed in this letter, please contact me at (202) 512-6253 or willemssenj@gao.gov.

Sincerely yours,

Joel C. Willemssen
Managing Director, Information Technology

---

[12]Pub. L. No. 111-148, 124 Stat. 119, March 23, 2010, as amended by the Health Care and Education Reconciliation Act of 2010, Pub. L. No. 111-152, 124 Stat. 1029, March 30, 2010. This legislation includes provisions intended to strengthen CMS's efforts to prevent fraud in the Medicare and Medicaid programs.

[13]GAO, *Medicare and Medicaid Fraud, Waste, and Abuse: Effective Implementation of Recent Laws and Agency Actions Could Help Reduce Improper Payments*, GAO-11-409T (Washington, D.C.: Mar. 9, 2011).

[14]National Correct Coding Initiative edits can detect claims with duplicate services delivered to the same beneficiary on the same date of service, such as more than one excision of a gallbladder for the same beneficiary. CMS provided guidance on how to implement this requirement through a state Medicaid directors' letter issued on September 1, 2010

Post-Hearing Questions for the Record
Submitted to Mr. Louis Saccoccio
From Senator Mark L. Pryor

"Harnessing Technology and Innovation to Cut Waste and Curb Fraud in Federal Health Programs"
July 12, 2011

1. Have you had a chance to review CMS's new pre-payment analytics program? If so, what are your initial thoughts on the program?
   Response from L. Saccoccio: NHCAA has not reviewed CMS's new pre-payment analytics program. Nevertheless, we believe that the use of pre-payment analytics in federal programs is certainly warranted and we applaud CMS's move to apply predictive modeling to Medicare fee-for-service claims. Considering that CMS pays 4.4 million claims each working day, predictive modeling seems the single best opportunity for CMS to move to a prevention strategy. Assessing risks through predictive modeling will allow CMS to begin to move away from the "pay and chase" practices of the past.

2. Your testimony focuses on the power of information sharing in the fight against fraud, but what can we do to make sure this shared information is not misused?
   Response from L. Saccoccio: The sharing of anti-fraud information has been recognized under federal and state law as a valid strategy for fighting fraud. Typical shared anti-fraud information consists of descriptions of emerging fraud trends and schemes, geographic areas of interest, billing codes being abused, and investigative techniques. When NHCAA members engage in information sharing activities, they do so under strict guidelines to which they are bound by written agreement. Moreover, the type of anti-fraud information shared between private and public payers does not contain patient information or personal health information of any kind, thereby eliminating any concerns under HIPAA privacy rules. NHCAA's information sharing guidelines could be used as a model to ensure that shared information is not misused, and we would be happy to share these guidelines with you.

3. The return on investment you described in your testimony on the Health Care Fraud & Abuse Control Program is extremely encouraging. In this challenging fiscal environment, legislation that improves our stewardship of taxpayer resources is vital. Do you see opportunities where that return on investment could be improved?
   Response from L. Saccoccio: CMS's current strategy of moving to a risk-based anti-fraud effort with a focus on prepayment fraud detection (i.e., preventing the dollars from going out the door in the first place) is the best opportunity for improving return on investment. This shift from a "pay and chase" mode of fraud fighting to one focused on predictive modeling and data analytics will require investment and a commitment by Congress and CMS. Purchasing and implementing new data systems is expensive. However, we believe that making this investment will generate significant returns in the coming years.

4. Do you see any emerging types of health care fraud that could be mitigated before they develop into a systemic problem? What should we be aware of on the horizon?
Response from L. Saccoccio: Fraud trends and schemes are constantly changing, developing, shifting, migrating and morphing. Those seeking to commit health care fraud are opportunistic by nature and will seek out weaknesses wherever they exist. We have claims systems that are based on tens of thousands of codes. Additionally, medical science creates an ever-expanding spectrum of new technologies, procedures and treatments. The key to staying ahead of the health care fraud curve is to create a health care anti-fraud program that is flexible and quickly adaptable. The predictive modeling program CMS has now activated holds great promise. If it functions as envisioned it should be able to identify emerging fraud trends and schemes and adjust quickly to address them.

Subcommittee on Federal Financial Management, Government Information, Federal Services and International Security
"Harnessing Technology and Innovation to Cut Waste and Curb Fraud in Federal Health Programs"

July 12, 2011

Louis Saccoccio, Executive Director, National Health Care Anti-Fraud Association

1) I understand that in the private sector, in credit cards, for instance, lenders tolerate a fraud rate of about one-tenth of one percent.
    a. Is there something intrinsic to health insurance or to federal health programs that means we must expect a higher rate of fraud?

Response from L. Saccoccio: NHCAA is not aware of the fraud rate used as a baseline in the credit card industry. Although we believe there are anti-fraud techniques and technologies used by the financial services industry that may have application for fighting health care fraud, fraud in health care is different from fraud in financial services because the health care delivery and payment system is so different from the system used for credit card transactions.

Foremost, health care is a personal service delivered to patients by a large and diverse range of health care providers. The goal of the system is to ensure that patients receive the care that they need. Regrettably, fraudsters often take advantage of that fact to perpetrate their fraud. Additionally, health care fraud is an exceptionally complex crime that manifests in countless ways, and that complexity is what makes health care fraud a challenge to detect. There are many variables at play. Considering that billions of medical claims are generated in the United States every year, the sheer volume of health care claims makes fraud detection a challenge. The government (at the federal and state levels) is a payer as is the private sector. Medicare alone pays 4.4 million claims per day to 1.5 million providers nationwide. Anyone in the system can conceivably try to commit fraud, and those committing fraud have the full range of medical conditions and treatments and the entire population of patients on which to base false claims. Detecting health care fraud often requires the knowledge and application of clinical best practices, as well as knowledge of medical terminology and specialized coding systems, including CPT and CDT codes, DRGs, ICD-9 codes, and the forthcoming ICD-10 codes. Clearly, health care fraud can be a challenging crime to prevent and detect. The perpetrators of this crime have proven themselves to be opportunistic, nimble and aggressive, adjusting schemes and tactics to avoid detection. Therefore, investing in and employing the most effective fraud prevention and detection techniques is critical to achieving success.

b. What role is played by the fact that beneficiaries suffer no direct loss – that it isn't their money on the line?
Response from L. Saccoccio: We believe the fact that most health care in this country is paid for either through employment based insurance or a government program, may lead beneficiaries to be less attuned to the reality of health care fraud. However, this doesn't mean that they would not be concerned if they realized the scope of the problem. Additionally, every taxpayer in the United States incurs a direct loss as a result of health care fraud, as does every employee who sees his or her health care premiums rise as a result of fraud. Remember that employees often pay a significant percentage of the total premium paid by employers for health insurance coverage. Moreover, health care fraud isn't just a financial crime. Health care fraud often harms patients and compromises the quality of care we all count on. Providing education to health care consumers (whether they are covered by a government program or through private insurance) about health care fraud and how they can protect themselves is an important part of an effective fraud-fighting effort.

2) You mentioned in your written testimony that fraudsters are opportunistic, that they adapt. Mr. Morris testified about fraudsters "pinging the system."
   a. How effective will anti-fraud tools be at identifying whole new kinds of scams?
   Response from L. Saccoccio: The real-time analytics tools that have been developed and continue to be improved will most certainly assist in identifying health care fraud scams and schemes. Analyzing data to identify weaknesses is important, but taking the action steps necessary to respond is equally important. These steps include things like applying new edits to the claims processing process, suspending payments when necessary, and taking into consideration variables such as geography, specialty area and the populations served when examining the data. But another critical step is the sharing of information about new scams and schemes among the health care fraud-fighting community. For example, if CMS identifies a new scheme, information about the scheme should be shared with other government and commercial payers. A collaborative approach that is committed to sharing key health care fraud trend information is another important way to protect our health care system as a whole.

   b. Does expanding the number of beneficiaries provide more opportunity for fraudsters?
   Response from L. Saccoccio: Most likely, yes. Each beneficiary represents a pool of available benefits that equate to potential health care claims. So more beneficiaries could equate to more potential exposure.

   c. Do you think having more money flowing through federal health programs will attract more fraudsters?
   Response from L. Saccoccio: For this, we refer to the infamous bank robber Willie Sutton who when asked by a reporter why he robbed banks responded, "because that's where the money is." Following this logic, having more money flowing through federal health programs will make them more attractive targets for those

seeking to commit health care fraud. This only argues for pursuing an aggressive anti-fraud agenda incorporating the latest anti-fraud detection technology, private-public payer information sharing, and committed law enforcement resources.

3) All of you alluded at one point or another in your testimony about problems stemming from your work with other organizations. Mr. Morris said that "contractors often disappoint us." Mr. Willemssen talked about holding states' "feet to the fire" about how they format their data. Dr. Budetti brought up the failings of contractors, states and providers. You have my support in overcoming these challenges. But leaving those aside for a moment:
   a. Can you each say what you see as the weakest part of the federal government's own performance in preventing fraud against Medicare and Medicaid?
   Response from L. Saccoccio: The lack of effective screening of providers entering the Medicare and Medicaid systems has been one of the most significant weaknesses in these programs. However, this weakness is now being addressed by CMS under the provisions of the Affordable Care Act and recently issued regulations requiring enhanced screening of providers based on the risk the providers potentially pose for fraud. NHCAA also commends the decision of the Secretary to consolidate program integrity functions for Medicare and Medicaid under one office, the Center for Program Integrity within CMS. NHCAA also believes that the consolidation of Medicaid data with Medicare data as part of the Integrated Data Repository (IDR)—a goal articulated by CMS at the hearing—will certainly enhance fraud prevention and detection efforts.
   b. What did the federal government not do right?
   Response from L. Saccoccio: NHCAA believes that the federal government 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 new strategy of a placing significant focus on pre-payment review is the right one.
   c. What specific part of federal performance and systems are ripest for improvement?
   Response from L. Saccoccio: NHCAA believes that consolidation of Medicare data and all state Medicaid program data in such a way that would allow for the application of predictive modeling and other analytics across this complete set of data is the area which holds the greatest promise for effective fraud fighting. Although not comprehensive of all payers, the consolidation of Medicare and Medicaid data for anti-fraud purposes would create the largest data base available to analyze for fraud patterns and trends. The results derived from this consolidation and analysis should then be available to all government programs and also shared with commercial payers. This would help prevent those committing fraud from migrating among payers since all payers would have access to information regarding the latest fraud trends and schemes.

CMS Fraud Detection System

(One PI and the Integrated Data Repository)

Costs to Date +	Lifecycle Costs to Completion	⇨	10-Year Fraud Avoidance
$161.1 Million	$183.9 Million		$21 Billion

Source: GAO

CMS Fraud Detection System

(One PI and the Integrated Data Repository)

10 Year Fraud Avoidance	$21.0 Billion
Costs to Date	$161.1 Million
Lifecycle Costs to Completion	$183.9 Million

Source: GAO

2010 IMPROPER PAYMENTS

- Medicare $47.9 Billion
- Medicaid $22.5 Billion

Chart 1