Statement of Louis Saccoccio

Executive Director

National Health Care Anti-Fraud Association

on

Improving Efforts to Combat Health Care Fraud

Before the

U.S. House Committee on Ways and Means

Subcommittee on Oversight

March 2, 2011

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

Good afternoon, Chairman Boustany, Ranking Member Lewis, 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 80 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 health coverage as an individual or through an employer, Medicare, Medicaid, TRICARE or other federal or state program.

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.

Health care fraud is a complex crime that can manifest in countless ways. There are many variables at play. The sheer volume of health care claims makes fraud detection a challenge. For example, Medicare alone pays 4.4 million claims per day to 1.5 million providers nationwide. Add to that the fact that fraud can conceivably be committed by anyone in the system, and that those committing fraud have the full range of medical conditions, treatments and patients on which to base false claims. Plus, 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. As a result, employing the most effective fraud prevention and detection techniques is critical to achieving success.

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 only a financial necessity; it is a patient safety imperative. For example, anti-fraud efforts identify and prevent unnecessary and potentially harmful medical care and procedures. Shockingly, 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 or dangerous medical procedures simply because of greed. Patients may also unknowingly receive unapproved or experimental procedures or devices.

Additionally, anti-fraud efforts identify dangerous prescription drug abuse by patients and overprescribing by some physicians. 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 that is best able to connect the dots and identify potentially fatal overprescribing by physicians and the resulting prescription drug abuse by patients.

Anti-fraud efforts also identify and 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. Victims of medical identity theft could receive the wrong (and potentially harmful) medical treatment, find that their health insurance benefits have been exhausted, become uninsurable for life insurance coverage, and 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.

My testimony today will focus on three issues which NHCAA believes are critical to successfully combating 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 importance of the new tools provided by the Patient Protection and Affordable Care Act, and the need for both private and public investment in anti-fraud activities.

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. We believe that government entities, tasked with fighting fraud and safeguarding our health system, and private insurers, responsible for protecting their beneficiaries and customers, can and should work cooperatively on this critical issue of mutual interest. Our experience has taught us that investigative information sharing 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, Medicaid Fraud Control Units, TRICARE, and other federal and state agencies come together to share information about developing fraud schemes and trends. Additionally, NHCAA'S Request for Investigative Assistance (RIA) process allows government agents to easily query private health insurers regarding their 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.

In addition to the NHCAA-sponsored information-sharing meetings, many U.S. Attorney Offices sponsor health care fraud task forces which 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.

[1] NHCAA Anti-Fraud Management Survey for Calendar Year 2009, National Health Care Anti-Fraud Association, June 2010.

The Department of Justice has developed guidelines for the operation of the Health Care Fraud & Abuse Control Program (HCFAC) established by HIPAA that 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."

One salient example which 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 public and private programs of millions of dollars, became 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.[3] These phantom providers across South Florida collected hundreds of millions of dollars from Medicare, Medicaid and other public programs.

During this time, the Department of Justice (DOJ) organized its first Health Care Fraud Strike Force in Miami-Dade.[4] While the government-led Strike Force was investigating, much of the information about these phantom providers was also being developed by private health insurers, much of it driven by information provided by beneficiaries – individuals who received

[2] See http://www.usdoj.gov/ag/readingroom/hcarefraud2.htm.
[3] See http://oig.hhs.gov/publications/docs/press/2007/PRSouthFlorida.pdf.
[4] See http://www.stopmedicarefraud.gov/heatsuccess/heat_taskforce_miami.pdf.

Explanation of Benefit forms from their public or private insurer for services they had not received.

Once information began to be shared between the public and private sectors, NHCAA member company investigators and others 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, and many checks returned as non-deliverable or stale dated. When these alleged providers were contacted by telephone, the phone calls typically reflected disconnected numbers or full voicemail boxes. Messages that were left by investigators were never returned. In the few instances when a live person answered the phone, they did not speak English (or pretended not to speak English), could not provide any information, or simply hung up.

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-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 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.

Despite the success of information sharing which 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 and encouraged 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 effective anti-fraud information sharing with the goal of increasing the effectiveness of this critical tool in the fight against health care fraud.

II. Data analysis and aggregation are essential tools in the health care fraud detection and prevention efforts of today and tomorrow.

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.[5] The complexity and size of the health care system, along with understandable concerns for patient privacy, probably make such a data base 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 Patient Protection &

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

Affordable Care Act. This section mandates an expanded "Integrated Data Repository" at CMS that will incorporate data from all federal health care programs:

- Medicare Parts A, B, C & D;
- Medicaid;
- CHIP;
- Health-related programs administered by the Secretary of Veterans Affairs;
- Health-related programs administered by the Secretary of Defense;
- Federal old-age, survivors, and disability insurance benefits established under Title II; and
- The Indian Health Service and the Contract Health Service program.

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 conducting law enforcement and oversight activities. This is a major step in the right direction for analyzing claims data in a way which will allow potential losses to be stemmed and emerging schemes to be identified 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 and then to 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, many private sector health insurers now devote additional resources to predictive modeling technology and real-time 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 then building models based on patterns that emerge from that data.

The federal government has also recognized the value of real-time 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 and among federal agencies. 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—this includes an expansion to two additional cities announced just last month. 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 three and a half years.[6]

Congress has demonstrated further 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, signed into law last September. 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.

The law describes a four-year implementation process and stipulates that the use of predictive analytics in fraud detection shall commence by July 1, 2011, in 10 states identified by the Secretary as having the highest risk of waste, fraud, or abuse in the Medicare fee-for service program. Importantly, CMS has indicated that it plans to accelerate the program, estimating that real-time analysis of national Medicare claims data "should be possible by 2012."[7] This

[6] 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.
[7] http://www.nextgov.com/nextgov/ng_20110209_7724.php#

ambitious push to implement predictive modeling signals the determination of CMS to root out fraud and safeguard our finite health care dollars.

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 it before it occurs.

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." Now, 14 years later, the documented success of HCFAC affirms the wisdom of making that investment. Published this past January, the HCFAC report for Fiscal Year 2010 shows a return on investment (ROI) of $4.90 returned 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. However, 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 Patient Protection and 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 potential fraudsters. Designed based on the potential risk of fraud by a certain category 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's important to be able to suppress it when and where it appears in order to limit its reach.

The ACA also creates the ability of the Secretary to suspend payments to a particular provider "pending an investigation of a credible allegation of fraud . . unless the Secretary determines there is good cause not to suspend such payments." 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 other state plan.

Among the many new anti-fraud provisions included as part of the health care reform package, additional funding for anti-fraud efforts was also a noteworthy inclusion. The law 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 investment, 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 a sound investment. 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, the recent regulatory decision to categorize anti-fraud activities undertaken by private insurers as simple "cost containment" in the recently published medical loss ratio (MLR) interim final rules 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 fraud prevention investments by private insurers. 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.

Conclusion

Health care fraud costs taxpayers billions of dollars every year, and 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. If there is such a thing as a

silver bullet for solving the health care fraud conundrum, enabling genuine information sharing among stakeholders is our best bet.

The schemes devised by perpetrators of health care fraud take many forms, and the perpetrators of fraud are opportunistic. As a result, we must stay vigilant and work to anticipate and identify the risks, and to 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. We encourage continued investment in both time and resources to exploring and implementing data consolidation and data mining techniques.

NHCAA is encouraged by the renewed federal emphasis given to fighting health care fraud. This hearing is an excellent example of this emphasis, 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 from our government health care programs, we urge decision makers to also recognize and encourage the important role that private insurers play in keeping our health care system healthy and free from fraud.

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