NHCAA
National Health Care Anti-Fraud Association®

Statement of Louis Saccoccio

Chief Executive Officer

National Health Care Anti-Fraud Association

on

The Use of Data Analysis to Identify Emerging Trends and Stop Medicare Fraud

Before the

U.S. House Committee on Ways and Means

Subcommittee on Oversight

March 24, 2015

NHCAA
National Health Care Anti-Fraud Association®

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

Good morning, Chairman Roskam, Ranking Member Lewis, and other distinguished Members of the Subcommittee. I am Louis Saccoccio, Chief Executive Officer of the National Health Care Anti-Fraud Association (NHCAA). I appreciate the opportunity to discuss with you how the use of data analytics can help protect seniors and taxpayers from Medicare fraud.

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 80 of our nation's most prominent private health insurers, along with nearly 130 federal, state and local 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 and abuse. The focus of this mission remains constant 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 three decades of experience focusing on this single issue. Health care fraud is a serious and costly problem that plagues our health care system, undermines our nation's economy and affects every patient and every taxpayer in America.

The extent of financial losses due to health care fraud in the United States, while not entirely known, is estimated to range from $75 billion[1] to an astounding $640 billion a year[2]. To be sure, the financial losses are considerable, but health care fraud is a crime that also directly impacts the quality of health care delivery. Patients are physically and emotionally harmed by it and as a result, fighting health care fraud is not only a financial necessity; it is a patient safety imperative.

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. Health care fraud is clearly not just a financial crime, and it is certainly not victimless.

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 Parts A and B alone process 4.5 million claims per day. Add to that the fact that fraud can conceivably be committed by any one of the 1.5 million providers of services and products in Medicare, and that those committing fraud have the full range of medical conditions, diagnoses, treatments and patients on which to base false claims. Plus, detecting health care fraud often requires the 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.

Plainly, health care fraud can be a challenging crime to prevent and detect. There is no single solution that will solve the problem and the landscape I describe demands that anti-fraud efforts be multi-faceted. A wide range of tools is essential to wage an effective and comprehensive battle against health care fraud.

[1] Young, Pierre L. and LeighAnne Olsen, "The Healthcare Imperative: Lowering Costs and Improving Outcomes." Institute of Medicine of the National Academies, 2010. http://www.nap.edu/openbook.php?record_id=12750.

[2] De Rugy, Veronique, and Jason J. Fitchner, "Is Federal Spending Too Big to be Overseen?" Mercatus Center, January 15, 2015. http://mercatus.org/publication/federal-spending-too-big-be-overseen.

My testimony today focuses on two elements which NHCAA believes are critical to successfully combating health care fraud. The first is the crucial role of data analytics, predictive modeling and other technology solutions in being able to prevent precious health care dollars from being lost to fraud. The second 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.

I. Data analysis and aggregation are essential tools in the health care fraud detection and prevention efforts.

The United States is projected to spend $3.21 trillion[3] dollars on health care in 2015 and generate billions of claims from health care service and product providers. Medicare alone accounts for $633 billion[4] in annual spending, representing more than 54 million[5] beneficiaries. Our nation's health care system hinges upon a staggering amount of data spread across the health care claim adjudication systems of numerous payers. 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.

We have learned that it is more cost effective to detect and prevent fraud prior to paying a fraudulent claim than to chase the lost dollars after the fact. The "pay and chase" model of combating health care fraud, while necessary in certain cases, is no longer tenable as the primary method of fighting this crime. 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.

One of Medicare's assets in terms of fraud detection is the enormous amount of data the program generates and collects. According to the most recent Health Care Fraud & Abuse Control

[3] Center for Medicare & Medicaid Services, Office of the Actuary. "National Health Expenditure Data, Projected." Accessed March 19, 2015. http://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/NationalHealthAccountsProjected.html.

[4] Center for Medicare & Medicaid Services, Office of the Actuary. "National Health Expenditure Data, Projected." Table 03 National Health Expenditures; Aggregate and per Capita Amounts. Accessed March 19, 2015. http://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/NationalHealthAccountsProjected.html.

[5] Center for Medicare & Medicaid Services, Office of the Actuary. "National Health Expenditure Data, Projected." Table 17 Health Insurance Enrollment and Enrollment Growth Rates. Accessed March 19, 2015. http://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/NationalHealthAccountsProjected.html.

Program (HCFAC) report, [6] the CMS Integrated Data Repository (IDR) contains a comprehensive and accurate set of Medicare provider, beneficiary and claims data from Medicare Parts A, B, and D dating back to January 2006. We believe that harnessing and applying analytics to that data could ultimately yield very powerful, game-changing results. The Centers for Medicare and Medicaid Services (CMS) has been dedicating significant resources to facilitate an operational shift to prepayment anti-fraud efforts, including the application of predictive models and other algorithms to Medicare claims through its Fraud Prevention System (FPS). The Small Business Jobs and Credit Act of 2010 established predictive analytics technologies requirements for the Medicare fee-for-service program.

As a result, CMS's Fraud Prevention System (FPS) was launched July 1, 2011. The technology used is similar to that used by credit card companies and financial institutions to detect and prevent fraud. The system, employed by CMS and its program integrity contractors, analyzes Medicare claims data, applying models and algorithms to identify providers and suppliers exhibiting a pattern of behavior that is indicative of potential fraud. Analysis through the FPS includes the use of rules to filter fraudulent claims and behaviors, the detection of anomalies in claims data, predictive assessment against known fraud cases (i.e., predictive modeling), and the use of associative link analysis. This process results in the assignment of risk scores on specific claims and providers which are prioritized for program integrity analysts to review and investigate.

CMS has submitted reports to Congress assessing the first[7] and second[8] years of implementation of the FPS that reveal significant gains and successes. It is quite understandable that many are anxious to see immediate, positive results from the investments already made in adopting predictive modeling and analysis. On that point, NHCAA would encourage continued patience regarding the use of predictive modeling and data analysis for combating fraud. It will take time to effectively refine and adjust the models for such a large and complex system as Medicare in

[6] U.S. Department of Justice, U.S. Department of Health and Human Services. The Department of Health and Human Services and The Department of Justice Health Care Fraud and Abuse Control Program Annual Report for Fiscal Year 2014. March 19, 2015.

[7] Centers for Medicare & Medicaid Services. Report to Congress: Fraud Prevention System, First Implementation Year. 2012. Accessed March 19, 2015. http://www.stopmedicarefraud.gov/fraud-rtc12142012.pdf

[8] Centers for Medicare & Medicaid Services. Report to Congress: Fraud Prevention System, Second Implementation Year. June 2014. Accessed March 19, 2015. http://www.stopmedicarefraud.gov/fraud-rtc06242014.pdf

order to realize the full potential that these powerful technologies offer. Despite the challenges, NHCAA strongly supports this effort.

Many private sector health insurers also have recognized the importance of data analytics to help detect potential fraud and devote resources to apply these tools to enhance their fraud prevention efforts. Seventy-seven percent of respondents to NHCAA's 2013 Anti-Fraud Management Survey[9] (a biennial survey of our private-sector members that aims to assess the structure, staffing, funding, operations and results of health insurer investigative units) indicated the use of some form of data analytics in their anti-fraud work, including predictive modeling, retrospective modeling, predictive scoring models, data mining queries, billing patterns and rules.

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

It is important to note, however, that while the use of data analytics is an important tool in the detection of fraud, it is not a panacea. Predictive analytics can generate leads for further inquiry and can help form the basis for the suspension of payments, but it has not been used as the sole basis for the suspension of payments by private health insurers without additional follow-up and corroboration.

Many of the data analysis and aggregation tools and systems being developed and brought to market are incredibly powerful and can produce potential leads at a pace that can quickly exceed what the finite investigative resources can handle. There is much attention being given to predictive modeling and prepayment analytics, and with good reason. However, the need for "boots on the ground" is as great as it has ever been. Technology professionals and data analysts will be in increasing demand as the use of prepayment technologies grows. And the leads and

[9] The National Health Care Anti-Fraud Association. NHCAA Anti-Fraud Management Survey for Calendar Year 2013. Washington, DC. 2014.

information developed by data analytics will continue to require, in many instances, skilled investigators and medical record reviewers with clinical backgrounds available to act on the information.

It is important that the anti-fraud units responsible for ensuring the integrity of our federal health care programs are staffed sufficiently to meet the challenge that fraud and abuse present. As we focus on the promise of technology, we mustn't overlook the vital need for smart, analytical, insightful, and committed fraud-fighting professionals. We must maintain a multi-prong approach to fighting health care fraud that strikes a balance between technological resources and human resources. So as we continue to extol the promise of cutting-edge technologies for combating health care fraud, waste and abuse, we must also champion the continued investment in human capital. We recommend that in its allocation of funding for anti-fraud efforts in Medicare and Medicaid, Congress recognize the necessity of building a workforce with the numbers, depth, specialization and skill necessary to be successful.

II. 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.

The vast majority of providers of health care services and products bill multiple payers, both private and public. For example, a health care provider may be billing Medicare, Medicaid, and several private health plans in which it is a network provider, and may also be billing other health plans as an out-of-network provider. However, when analyzing this provider's claims for potential fraud or abuse, each payer is limited to the claims it receives and adjudicates and is not privy to claims information collected by other payers.

Currently, there exists no single repository of all health care claims similar to what exists for property and casualty insurance claims.[10] The complexity and size of the health care system, along with understandable concerns for patient privacy, likely make such a database impracticable. Nevertheless, the absence of such a tool limits the effectiveness with which health

[10] ISO ClaimSearch. See https://claimsearch.iso.com

claims (housed in the discrete databases of individual payers) can be analyzed to uncover potential emerging fraud schemes and trends.

In this environment, fraudsters bank on the assumption that payers are not working together to collectively connect the dots and uncover the true breadth of a scheme. Health care fraud does not discriminate between types of medical coverage. The same schemes used to defraud Medicare and Medicaid migrate to private insurance, and schemes perpetrated against private insurers make their way into government programs. It is precisely this reason why the sharing of preventive and investigative information among payers is crucial for successfully identifying and preventing health care fraud. Payers, whether private or public, who limit the scope of their anti-fraud information to data from their own organization or agency are taking an uncoordinated and piecemeal approach to the problem.

Our experience as a champion and facilitator of anti-fraud information exchange has taught us that it is very effective in combating health care fraud. Government entities, tasked with fighting fraud and safeguarding public programs, and private insurers, responsible for protecting their beneficiaries and customers, can and should work cooperatively on this critical issue of mutual interest.

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

The Department of Justice (DOJ) also recognizes the benefit of private-public information sharing. Many U.S. Attorney Offices sponsor health care fraud task forces that hold routine information-sharing meetings, and when invited to do so, private insurers often participate in these meetings to gather and offer investigative insight. In fact, eighty-seven percent of respondents to NHCAA's 2013 Anti-Fraud Management Survey[11] report that they share case information at law enforcement-sponsored health care fraud task force meetings.

Additionally, DOJ developed guidelines for the operation of the Health Care Fraud & Abuse Control Program (HCFAC) established by HIPAA which provide a strong basis for information sharing. The "Statement of Principles for the Sharing of Health Care Fraud Information between the Department of Justice and Private Health Plans"[12] acknowledges the importance of a coordinated program, bringing together both the public and private sectors in the organized fight against health care fraud.

Despite DOJ's recognition of information sharing as an anti-fraud tool, NHCAA, along with other organizations, saw the need to improve and expand the cooperation and anti-fraud information sharing between the private and public sectors. This concept was a topic of focus during the National Health Care Fraud Prevention Summit hosted by the Department of Justice and the Department of Health & Human Services in January, 2010, in which NHCAA and numerous private insurers participated. This summit set into motion a determined effort to develop and establish a more formalized partnership between government agencies and private sector health insurers. It was envisioned that such a partnership would facilitate anti-fraud information exchange by creating a process to exchange not just investigative information, but to allow the exchange of private and public payer data in a way that could lead to earlier and more effective detection and prevention of fraud.

[11] The National Health Care Anti-Fraud Association, The NHCAA Anti-Fraud Management Survey for Calendar Year 2013 (Washington, DC, NHCAA, July 2014).

[12] United State Department of Justice. Statement on the Principles for the sharing of Healthcare Fraud Information. Updated Sept 2014. See http://www.usdoj.gov/ag/readingroom/hcarefraud2.htm.

After more than two years of discussions and meetings involving several interested parties, including NHCAA, the Healthcare Fraud Prevention Partnership (HFPP) was formally announced on July 26, 2012, at the White House. The HFPP is a joint initiative of the U.S. Department of Health & Human Services and the Department of Justice. It is a voluntary public-private partnership between the federal government, state officials, private health insurance organizations, and health care associations which aims to foster a proactive approach to detect and prevent health care fraud across all public and private payers. NHCAA believes that the HFPP is the necessary next step that takes the information sharing work NHCAA has done, and will continue to do, to a higher level of complexity and effectiveness through the sharing of actual payer data through designated, targeted studies of particular fraud risk areas.

The HFPP has an Executive Board that provides strategic direction and input for the partnership and shares information with the leadership of member organizations. In addition there are two committees:

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

While the HFPP does not intend to create a national-level all-claims database, it has established several principles and goals that hinge significantly upon the concept of information and data sharing. HFPP partners will work together to combat fraud by:

- Engaging in value-added data-exchange studies between the public and private sector partners.
- Leveraging analytic tools and technologies against this more comprehensive data set.

The partnership and its committees employ a “study-based” approach for data sharing, whereby studies are proposed, planned, executed and analyzed. Smaller, more targeted groups of partners are typically convened to conduct specific studies. An important aspect of the HFPP is the use of a Trusted Third Party (TTP) to serve as a data-exchange entity for the studies. As envisioned, the TTP conducts HFPP data exchanges, research, data consolidation and aggregation, reporting and analysis. The TTP does not share the source of the data during an exchange in order to keep the identity of the data source confidential.

The HFPP has already completed several studies associated with fraud, waste or abuse that have yielded successful results for participating partners, including studies examining “false store fronts” or “phantom providers,” entity revocation/termination lists, misused codes and top billing pharmacies. The misused codes study, for example, examined claim codes, or claim code combinations, that HFPP partners had assessed to be frequently associated with fraud, waste or abuse in the previous six to 12 months, and were associated with large-dollar claims or high utilization. The resulting data exchange proved successful. Schemes and codes that were not thought to be problematic by certain partners were highlighted in the exchange results. The process also confirmed known schemes and misused codes. Further analysis will be conducted and sharing of the results will continue.

At present, the HFPP has nearly 40 partners, including CMS, and it will continue to grow. Ideally the HFPP will foster a national scope by encouraging the participation of eligible public and private entities in the health care industry that are willing and able to meaningfully contribute health care data.

While NHCAA and the HFPP work to promote and improve the effectiveness of data exchange and anti-fraud information sharing, many NHCAA members remain reluctant to fully participate in anti-fraud sharing activities for fear of the potential legal risk such sharing raises. For example, some health insurers are hesitant to share data or information that could lead to litigation brought by health care providers who may be the subject of the shared data or information.

While some states provide immunity for fraud reporting (typically to law enforcement and regulatory agencies, although protections, as well as reporting requirements, vary by state), there exists no clear federal protection for insurers that share information with one another about suspected health care fraud. The absence of such protection creates a chilling effect that leads some organizations to determine that the risk of sharing information outweighs the potential benefit. Although the decision to avoid the risk may seem to make sense to a particular company, the decision results in a negative impact on the overall fight against health care fraud.

In 1996, the Government Accountability Office (GAO) conducted a study titled, "Health Care Fraud: Information-Sharing Proposals to Improve Enforcement Efforts."[13] It examined the issue of immunity and included views and recommendations from NHCAA. The GAO found broad support among federal and state officials, as well as insurers and state insurance commissioners, for a federal immunity statute. Several federal officials interviewed for the report recommended immunity for insurers sharing fraud-related information with other insurers. It's worth noting that this report also examined the idea of establishing a centralized health care fraud database to enhance information sharing and support enforcement efforts.

Based on this report, there seemed to be wide support for federal protections for sharing anti-fraud information. However, the legislation that would have implemented these ideas was not enacted (S. 1088, 104th Congress[14]). Now, nearly 20 years later, we remain essentially in the same situation with regard to immunity. However, the difference is that rather than spending $1 trillion[15] annually on health care as we did 20 years ago, today we spend $3.21 trillion.

NHCAA believes that we should remove unnecessary obstacles that inhibit fraud fighting efforts, and that providing protections for individuals and entities that share information and data concerning suspected health care fraud is a reasonable and prudent step to take. The GAO report

[13] Health Care Fraud: Information-Sharing Proposals to Improve Enforcement Efforts, the Government Accountability Office, May 1996. http://www.gpo.gov/fdsys/pkg/GAOREPORTS-GGD-96-101/html/GAOREPORTS-GGD-96-101.htm

[14] Senate Bill 1088, 104th United States Congress. "Health Care Fraud and Abuse Prevention Act of 1995," Sponsor: Senator William Cohen. http://www.gpo.gov/fdsys/pkg/BILLS-104s1088is/pdf/BILLS-104s1088is.pdf

[15] National Health Expenditure Data, historical 1960-2012, Centers for Medicare and Medicaid Services, Office of the Actuary. http://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/Downloads/tables.pdf

discussed above remains relevant to this discussion and may offer worthwhile models to consider.

Conclusion

Health care fraud costs taxpayers billions of dollars every year, and fighting it requires focused attention and a commitment to innovative solutions. There is no silver bullet for defeating health care fraud. A winning fraud prevention strategy for Medicare must be multi-faceted. We believe the following are all necessary components of a successful anti-fraud program:

- The use of data analytics and aggregation;
- A commitment to sharing anti-fraud information among payers;
- The application of rigorous screening processes for providers entering the program;
- The development and adoption of innovative investigative methodologies;
- The continuous investment in an adequate and skilled anti-fraud workforce;
- The aggressive pursuit of criminal prosecutions and the imposition of civil penalties for those who commit fraud; and
- The education of consumers and providers.

The schemes devised by perpetrators of health care fraud take many forms, and those perpetrators are exceptionally opportunistic. As a result, we must stay vigilant and strive to anticipate and identify the risks, and develop strategies to meet them. 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 support continued investment in both time and resources to enhance and implement data consolidation and data mining techniques, including predictive modeling, under Medicare.

Additionally, anti-fraud information and data sharing among private and public payers of health care are critically important and should be encouraged and strengthened. Health care payers cannot work in isolation and expect to be successful in detecting and preventing health care fraud. The establishment of federal protections for those individuals and entities engaged in anti-fraud information and data sharing would be a major step in encouraging this essential activity, and also would lend strong support for the growth and success of the HFPP as it moves forward. In our view, the HFPP signals a new era of private-public collaboration full of possibility, representing as a significant step in preventing fraud in Medicare and our entire health care system generally.