NHCAA
National Health Care Anti-Fraud Association®

Statement of Louis Saccoccio

Chief Executive Officer

National Health Care Anti-Fraud Association

on

"Preventing Medicare Fraud:

How Can We Best Protect Seniors and Taxpayers?"

Before the

United States Senate

Special Committee on Aging

March 26, 2014

NHCAA
National Health Care Anti-Fraud Association®

Testimony of:

Louis Saccoccio

Chief Executive Officer

National Health Care Anti-Fraud Association

Good afternoon, Chairman Nelson, Ranking Member Collins and other distinguished Members of the Committee. 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 to best protect seniors and taxpayers from Medicare fraud.

Established in 1985, NHCAA is the leading national organization focused exclusively on combating health care fraud and abuse. NHCAA has remained as a private-public partnership since its founding, making it uncommon among associations. Our members comprise more than 80 of the nation's most prominent private health insurers, together with nearly 120 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.

The NHCAA mission is straightforward: To protect and serve the public interest by increasing awareness and improving the detection, investigation, civil and criminal prosecution and prevention of health care fraud and abuse. Our commitment to this mission is the same regardless of whether a patient has private health care coverage or is a beneficiary of Medicare, Medicaid, or any other federal or state program. In my testimony today I draw upon our organization's nearly 30 year history of combating health care fraud.

On a national level, fraud hampers our health care system and undermines our nation's economy. The United States is projected to spend $3.1 trillion[1] dollars on health care in 2014 and generates billions of claims from health care service and product providers every year. Medicare alone accounts for $635 billion[2] in annual spending. On an individual level, no one is left untouched by health care fraud; it is a serious and costly problem that affects every patient and every taxpayer across our nation. The extent of financial losses due to health care fraud in the United States, while not entirely known, is estimated to range in the tens of billions of dollars or more. To be sure, the financial losses are considerable, but those losses are compounded by numerous instances of patient harm -- unfortunate and insidious side effects of health care fraud that impact patient safety and diminish the quality of our medical care. Health care fraud is not just a financial crime, and it is certainly not victimless.

Health care fraud 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. Medicare Parts A and B alone pay 4.5 million claims every 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 application of knowledge of medical and clinical best practices and terminology, along with a proficiency in arcane coding systems including CPT, CDT and HCPCS codes, DRGs, ICD-9 codes, and the forthcoming ICD-10 codes.

[1] National Health Expenditure Projections 2012-2022, 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/Proj2012.pdf
[2] Ibid.

The landscape I describe demands that anti-fraud efforts be multi-faceted. There is no single solution that will solve the problem. A wide range of tools is necessary to wage an effective and comprehensive battle against health care fraud -- methods such as the use of data analytics and predictive modeling; the application of rigorous provider screening processes; the development of innovative investigative methodologies; the maintenance of a skilled and sufficient anti-fraud workforce; and the education of consumers and providers are all necessary components of an effective anti-fraud program.

In addition to the methods listed above, there is another concept that is essential to being able to successfully fight health care fraud. The remainder of my comments will concentrate on this concept -- one that has been the focus of the work of NHCAA for nearly three decades and that offers our best chance of success at preventing fraud. This concept is anti-fraud information sharing. NHCAA is convinced that the exchange of anti-fraud information between and among public and private payers of health care is critical to the success of anti-fraud efforts and should be encouraged and strengthened.

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. 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.

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.[3] The complexity and size of the health care system, along with understandable concerns for patient privacy, likely make such a database impracticable. Nevertheless, the absence of such a tool limits the effectiveness with which health claims (housed in the discrete databases of individual payers) can be analyzed to uncover potential emerging fraud schemes and trends.

In this environment, fraudsters bank on the assumption that payers are not working together to collectively connect the dots and uncover the true breadth of a scheme. 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.

For example, 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

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

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 safeguard and recover funds that would otherwise be lost to fraud.

The Department of Justice (DOJ) has also recognized the benefit of private-public information sharing. For example, many U.S. Attorney Offices sponsor health care fraud task forces that hold routine information-sharing meetings, and when invited to do so, private insurers often participate in these meetings to gather and offer investigative insight. In fact, eighty-nine percent of respondents to NHCAA's 2011 Anti-Fraud Management Survey[4] (a biennial survey of our private-sector members that aims to assess the structure, staffing, funding, operations and results of health insurer investigative units) report that they share case information at law enforcement-sponsored health care fraud task force meetings.

Additionally, DOJ developed guidelines for the operation of the Health Care Fraud & Abuse Control Program (HCFAC) established by HIPAA which provide a strong basis for information sharing. The "Statement of Principles for the Sharing of Health Care Fraud Information between the Department of Justice and Private Health Plans"[5] acknowledges the importance of a coordinated program, bringing together both the public and private sectors in the organized fight against health care fraud.

[4] The National Health Care Anti-Fraud Association, The NHCAA Anti-Fraud Management Survey for Calendar Year 2011 (Washington, DC, NHCAA, July 2012) p. 44.
[5] See http://www.usdoj.gov/ag/readingroom/hcarefraud2.htm.

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 and steady effort to develop and establish a more formalized partnership between government agencies and private sector health insurers. It was envisioned that such a partnership would facilitate anti-fraud information exchange 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.

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 anti-fraud associations, like NHCAA, which aims to foster a proactive approach to detect and prevent health care fraud across all public and private payers. NHCAA believes that 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 in designated studies.

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.

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.

At present, the HFPP has more than 30 partners, including several private insurers. Formal steps are being taken to expand the partnership and 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 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.

- Providing a forum for business and government leaders and subject matter expert members to share successful anti-fraud practices and effective methodologies and strategies for detecting and preventing health care fraud.

The HFPP has already conducted a few initial studies, including one on misused codes and fraud schemes. Misused codes included those claim codes, or claim code combinations, that partners had assessed to be frequently associated with fraud, waste or abuse in the last 6 to 12 months, and associated with large-dollar claims or high utilization. Fraud schemes referred to descriptions of major fraud schemes in the last 6 to 12 months with an associated high-dollar amount. 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.

An important aspect of the HFPP is the use of a Trusted Third Party (TTP) to serve as a data-exchange entity. As envisioned, the TTP will conduct HFPP data exchanges, research, data consolidation and aggregation, reporting and analysis. The TTP will not share the source of the data during an exchange in order to keep the identity of the data source confidential. This concept is similar to one that has been employed successfully for many years through the Federal Aviation Administration's (FAA) Aviation Safety Reporting System (ASRS). The ASRS is a voluntary system run by the National Aeronautics and Space Administration (NASA) that allows pilots and other airplane crew members to confidentially report near misses and close calls in the interest of improving air safety. The confidential and independent nature of the ASRS is vitally

important. Reports that are submitted are stripped of identifying information and an immunity policy is in place that encourages submission of all safety incidents and observations.

While NHCAA and the HFPP work to promote and improve the effectiveness of data 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. This reluctance is demonstrated by the fact that only 40% of NHCAA health insurance company members enter information about their open fraud investigations into NHCAA's SIRIS database. This 40% rate is in stark contrast to the 95% of the same members who search the database for information entered by other companies. Clearly, the interest in receiving anti-fraud information exists; however, the willingness of a company to share its own information is clearly hampered by the perceived risks involved.

While many 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 federal protection for insurers that share information with one another about suspected health care fraud. As demonstrated by the percentages mentioned above, 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.

For many years, NHCAA has supported immunity protections for the sharing and reporting of health care fraud-related information (when provided in good faith and without malice). In May of 1996, the Government Accountability Office (GAO) conducted a study titled, "Health Care Fraud: Information-Sharing Proposals to Improve Enforcement Efforts."[6] The study examined the issue of immunity and includes NHCAA's views and recommendations. 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[7]). 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[8] annually on health care as we did 20 years ago, today we spend $3.1 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 discussed above remains relevant to this discussion and may offer worthwhile models to consider.

---

[6] 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

[7] 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

[8] 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

Conclusion

There is no silver bullet for defeating health care fraud. A winning fraud prevention strategy for Medicare must be multi-faceted. We believe one of the most important aspects of health care fraud prevention is anti-fraud information and data sharing among private and public payers of health care, which should be encouraged and strengthened. Health care payers, including the Medicare program, 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 and holds great promise as a significant step in preventing fraud in Medicare.

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