



Testimony

for

**House Ways and Means Committee
Subcommittee on Oversight**

Health Plan Programs to Combat Fraud, Waste, and Abuse

by

**Karen Ignagni
President and CEO
America's Health Insurance Plans**

March 2, 2011

I. Introduction

Chairman Boustany, Ranking Member Lewis, and members of the subcommittee, I am Karen Ignagni, CEO of America's Health Insurance Plans (AHIP), which is the national association representing health insurance plans that provide coverage to more than 200 million Americans. Our members offer a broad range of health insurance products in the commercial marketplace and also have demonstrated a strong commitment to participation in public programs.

We appreciate this opportunity to testify on the important role private health insurance plans play in preventing and detecting fraud, waste and abuse. As increasingly sophisticated schemes targeting scarce health care dollars are devised, an effective fraud-fighting strategy is a critical issue for health plans and the enrollees they serve. Recognizing that fraud has far-reaching implications both for health care costs and quality, our members have demonstrated strong leadership in continually developing new and innovative strategies to combat fraud, while also serving as valuable partners for federal and state law enforcement officials.

Our testimony addresses two issues:

- How health plans' fraud detection units are using cutting-edge techniques to identify practices leading to substandard care – including overuse, underuse, or misuse of medical treatment; and
- Our suggestions for improving fraud detection and prevention in both public and private programs.

II. How Health Plans Use Cutting-Edge Techniques in Detecting and Preventing Fraud

Health care fraud is not a victimless crime; it has an enormous adverse impact on quality while also imposing higher costs on consumers, employers, and taxpayers. Health plans have developed effective fraud prevention and detection programs as part of a broad-based strategy for improving health outcomes and achieving the optimal use of health care dollars. Moreover, the success of health plans' fraud prevention initiatives is evidenced by the fact that government programs now are incorporating these innovative private sector practices.

Health plans fight fraud by operating special investigations units (SIUs) that are staffed with qualified personnel, including many with statistical, medical, and law enforcement experience. These SIUs perform sophisticated tasks that include investigating claims, coordinating with law enforcement personnel, training in-house personnel to identify and report possible fraud, developing and using sophisticated software to identify possible fraudulent claims, initiating civil actions seeking recovery of improper claims payments, and preparing “evidence packages” of suspected fraudulent providers for the benefit of law enforcement entities. Health plans also are vigilant about the credentialing of providers to be included in their networks, and continue to monitor the maintenance of those credentials to assure quality.

Health plans use sophisticated fraud detection software to identify individuals who provide care using false credentials, deliver medically unnecessary services, or make treatment decisions based on illegal referral relationships. Health plans place a high priority on identifying providers who perform or order medically unnecessary procedures or whose practice patterns lead to the delivery of inappropriate or unnecessary care that can threaten the health and safety of patients.

The intensity of health plan fraud prevention programs is highlighted in a recent AHIP Research Brief,¹ entitled “Insurers’ Efforts to Prevent Health Care Fraud.” Based on data collected in a survey of health plans serving 95 million enrollees, the report details how health plan programs prevent and detect fraud, including how they marshal resources to identify and prevent potential fraud, *rather* than “paying and chasing” after the fact. Indeed, the report emphasizes that deterrence may generate the greatest impact from insurers’ anti-fraud programs. The knowledge that health plans have robust anti-fraud measures and controls likely prevents many inappropriate billings or claims from occurring in the first place.

Four Steps in Preventing Inappropriate, Unnecessary Billing or Falsification of Medical Records

The specific tools that health plans use to assure integrity and detect the delivery of inappropriate or unnecessary care vary by company, but usually include the following four categories of activities:

¹ AHIP Center for Policy and Research, Insurers’ Efforts to Prevent Health Care Fraud, January 2011.

- **Identifying potential fraud:** The first step is for the anti-fraud units to develop and use procedures to identify and detect suspect claims. The goal is to have this occur up-front, and to identify patterns of performing, ordering, or delivering medically unnecessary procedures before the claim is paid. Identification of such claims can come from the health plan's own systems, where software detects aberrant billing patterns, using data analysis and other analytics techniques. Information on suspected cases of fraud also is obtained from law enforcement agencies, as well as from the National Health Care Anti-Fraud Association (NHCAA). Members of the public also play an important role, as our members' fraud "hotlines" encourage patients as well as providers to report information that helps identify fraud in real-time, before payments are made.
- **"Tagging" suspected cases of fraud:** The second step is for such suspicious claims to be "tagged" for further review before payment. Health plans have been steadily expanding their use of technology to increase their capabilities for detecting fraud, such as through the implementation of electronic "smart flags" or "tags" that quickly identify potentially false or misleading diagnoses, as well as "mining" of claims databases to find suspected cases. A particularly important strategy is the widespread use of predictive modeling to identify suspected cases of fraud by particular providers, often for a more intensive review before claims are paid. For example, a Texas pain clinic case raised red flags based on the enormous quantity of painkillers prescribed, as well as the continual, regular submission of bills every two weeks – bills for services that turned out to be illusory, since patients were required to sign blank medical notes to "prove" they were at the clinic and received the injections. Claims are "scored" to identify those that have a high probability of fraud, and compared to historical claims data to catch statistical "outliers." An example would be clearly excessive claims, such as one physician submitting claims for 20 hours or more of work every day of the year. Such predictive modeling is an important tool when state prompt pay laws often require payments to providers to be made quickly, before a full investigation can be undertaken.
- **Investigating and auditing suspected fraudulent claims:** The next step includes extensive investigation and auditing of suspected claims, comprising medical record review, clinical investigations, and coordination with clinical services departments (including in-house doctors and nurses) to develop appropriate medical opinion of the legitimacy of the claim. Companies are hiring and training personnel to become more knowledgeable about health care fraud and prevention, and involving their auditors in working across multiple

disciplines. Those consulted in this review might include not only clinical and pharmacy personnel, but also state and federal law enforcement officials.

- **Taking action on suspected fraud:** While claims found to be appropriate and accurate would then be paid, claims that are suspected to be fraudulent would be handled on a case-by-case basis. In certain cases, facts that may constitute violations of law would be escalated by referral to a federal or state law enforcement agency (including the FBI and State Attorneys General) through development of what our special investigations units call an “evidence package” detailing the possible fraud. Health plans’ data, including extensive computer runs, are valuable evidence for prosecutors in subsequent trials.

Health Plan Techniques as Models

Health plans’ cutting-edge techniques have been recognized as effective and have served as a model for government programs. For example, the Medicare fee-for-service system historically has taken a “pay and chase” approach – meaning that often millions of dollars are paid *before* fraud is identified, thus making it difficult to recover funds that already have been lost to fraud. Now, however, significant efforts are underway to incorporate some of the best ideas of the private sector, including up-front detection and prevention, authority to suspend payments to a suspected provider, and enhanced data-sharing.

- **Protecting Patients From Unlicensed or Unqualified Providers**

Health plan credentialing programs are designed to ensure that a particular provider is licensed, has appropriate credentials, does not have a criminal record, and has not been disciplined or otherwise sanctioned. Consistent with the need for up-front detection and prevention, government programs are adopting the intensive credentialing of providers that health plans perform before they are allowed to be included in networks. To counter the historical ability of unscrupulous providers to participate in public programs simply by supplying a tax ID number and a “license,” the Affordable Care Act (ACA) beefs up CMS’s program integrity activities to mirror credentialing efforts employed by the private sector. Under the ACA, the Secretary of HHS is given the authority to impose enhanced oversight and screening measures, including licensure checks, background checks and site visits, on providers enrolled in Medicare, Medicaid, and the Children’s Health Insurance Program (CHIP). Indeed, for those providers deemed even a “limited” risk of fraud, waste and abuse, beginning on March 23, 2011, newly enrolling providers would be subject not only to verification, but also to database checks on a

pre- and post-enrollment basis to ensure that they continue to meet the enrollment criteria for their type of provider.

- **Suspending Payments When Fraud is Detected**

Health plans typically have included in their contracts with providers the ability to suspend payments for fraud if improper billing practices are suspected – an ability critical to maintaining quality standards and ensuring that enrollees receive appropriate health care services and treatments. In addition, health plans’ contracts typically allow them to recover funds from providers who engage in improper and/or inappropriate billing practices, and even close the provider’s panel or terminate the provider (in addition to recovering overpayments) if the provider intentionally engages in improper billing practices. The new anti-fraud provisions incorporate these practices into government programs and now allow the suspension of payments to providers in the case of “credible evidence of fraud” for more than 180-days.

- **Data Sharing**

In addition to thorough credentialing and oversight of providers, plus suspension of payments in cases of suspected fraud, another important technique in health plans’ arsenal against fraud is *data-sharing both internally and externally*. Often, fraud investigations combine the expertise of a number of experts, including clinical investigators, auditors, and physicians and, as necessary, outside experts to prevent and detect fraud through a coordinated approach. For example, fraud prevention programs that focus on the diversion, misuse and inappropriate prescribing of narcotic drugs (e.g., OxyContin) typically include close collaboration between the fraud unit’s investigators and a plan’s clinical services department to address the intersection between abusive conduct and quality of care.

In terms of sharing data outside of the plan, the NHCAA, founded in 1985 by a coalition of private health insurers and government officials, has been instrumental in assisting our members to pool information and identify the latest fraud and abuse trends and schemes. So too, in the public sector, the HHS Office of Inspector General (OIG) now has new authority to access data for oversight and law enforcement activities; for example, the OIG now can enter into data-sharing agreements with the Social Security Administration, as well as expand its data-bank to include claims and payment data from other programs, such as the Veterans Administration and the Department of Defense. As we highlight in our recommendations below, we believe that these initiatives are crucial but that more work needs to be done to facilitate information sharing with the private sector.

- **Preventing Identity Theft**

When a patient borrows a friend's identity to obtain insurance coverage, harm can result to the real beneficiary of that insurance policy, who may be tagged with the wrong blood type or be identified as having those medical conditions for which the friend received treatment. There also have been instances where patients have stolen a doctor's billing identity, as one health plan discovered when its computer software revealed that a psychiatrist's identity was being used to allegedly bill for seeing an impossible 63 patients in a single day.² The private sector is exploring technologies to combat these examples of medical identity theft, perhaps by methods such as biometrics incorporated in a patient's insurance card to assure that the patient is present.³ Indeed, a bill introduced in 2010, H.R. 5044, the "Medicare Fraud Enforcement and Prevention Act," mirrored that idea, providing for a pilot program that implements biometric technology to ensure that individuals entitled to Medicare benefits are "physically present at the time and place of receipt of certain items and services."

- **Detecting Substance Abuse**

A current fraud and abuse initiative that literally has "life and death" significance for patients is the growing problem of substance abuse – both identifying members who are battling a substance abuse problem, or abusing their pharmacy benefit, as well as investigating those prescribers who exploit member addiction for financial gain. Our members are seeing an increase in the prescribing of pharmaceuticals, especially controlled substances such as painkillers, for a non-legitimate medical purpose in violation of the law. Health plans employ data analysis to flag those who may be prescribing inappropriately or members who may be battling a substance abuse problem. In the latter case, the plan's medical personnel will organize substance abuse treatment.

III. Recommendations for Improving Fraud Prevention and Detection in Both Public and Private Programs

Looking ahead, additional measures are needed to improve the prevention and detection of fraud. To meet this goal, we offer the following four recommendations for the Committee's consideration.

² Appleby, J., "Medical claims 'mined' to find fraud: Use of detection software spreads," USA Today, November 7, 2006.

³ Harnish, A., "Analytics Improving Insurers' Claims Fraud Detection Efforts," Insurance and Technology, August 16, 2010.

Recognize the Role of Fraud Prevention and Credentialing Activities in Quality Improvement

Given the role that health plan fraud prevention and detection programs and credentialing have played in establishing effective models for public programs, improved data for law enforcement, and successful prevention efforts, how these programs are categorized under the implementation of the medical loss ratio (MLR) provision of the ACA should be reevaluated.

The specific issue relating to fraud prevention is that the MLR Interim Final Rule (IFR) states that it adopts the recommendations made by the National Association of Insurance Commissioners (NAIC). In turn, the NAIC's recommendations only provide a credit for fraud "recoveries" – i.e., funds that were paid out to providers and then recovered under "pay and chase" initiatives. It does not include the cost of developing and administering anti-fraud programs that detect fraud before claims are paid and in the process help to protect consumers, purchasers, and patients. As a result, the IFR would penalize health plans for committing resources to innovative programs that prevent and detect fraudulent conduct or prevent the delivery of unnecessary services or care.

By taking this approach, the MLR IFR's treatment of fraud prevention expenses works at cross purposes with new government efforts to emulate successful private sector programs, such as those described here, and it is at odds with the broad recognition by leaders in the private and public sectors that there is a direct link between fraud prevention activities and improved health care quality and outcomes.

Similarly, the MLR IFR categorically excludes provider credentialing from the definition of activities that improve health care quality. As now recognized in government programs, provider credentialing is a critical function that helps ensure, among other things, that the providers from whom an individual or family seeks care are properly licensed and qualified – thereby contributing directly to patient safety.

We would urge a reconsideration of potential options for the treatment of fraud prevention and credentialing programs. Excluding these expenses is contrary to the health reform goals of developing a system to deliver consistently high quality care, optimizing the use of health care resources, and enhancing anti-fraud cooperation between private and public entities.

Enhance Information Available to the Private Sector Through Increased Data-Sharing With the Public Sector

Partnerships that promote information sharing between the private and public sectors are crucial to the success of fraud prevention efforts. Indeed, such partnerships were envisioned under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which resulted in federal guidelines that encouraged the sharing of information among federal, state and local law enforcement entities, and recognized the large stake that health plans have as well in anti-fraud initiatives. Unfortunately, the HIPAA vision has not been fulfilled with respect to information sharing from public to private programs, likely hampered in part by the misperception by some federal and state agents that they lack the authority to share health care fraud information with their private counterparts.

Regardless of the specific reasons, there is much more to do in this area to make information sharing a two-way street between public and private programs, especially given that health plans are often administrative partners in public programs such as Medicare. Health plans are valuable partners for prosecutors for several reasons. They have advanced information technology infrastructures that can give law enforcement agencies a 360 degree view of a particular provider's behavior. Plans also can track clinical information across multiple providers, whether individual or institutional, and often in multiple geographic locations. That information can highlight the "outliers," whether in the form of overbilling, billing for treatments not rendered, or falsifying a diagnosis. In addition, plans often have access to drug utilization review systems that can determine when an individual is committing fraud by filling multiple prescriptions for a controlled substance, or when a prescriber is prescribing doses of such substances that far exceed normally expected amounts.

One of HHS' strategic principles⁴ for fighting health care fraud is to establish new partnerships with the private sector to share information and strategies for detecting and preventing fraud. We strongly support that direction, including further efforts by federal and state agencies to clarify the permissibility, as well as the beneficial nature, of sharing health care fraud-related information with private insurers engaged in fighting fraud.

⁴ HHS Testimony before House Appropriations Committee, March 4, 2010.

Ensure the Inclusion of Private Sector Government Program Components In Federal Cases

Our health plans commend the comprehensive federal Health Care Fraud and Abuse Control Program, begun in 2009 under the direction of the Attorney General and the Secretary of HHS, for its anti-fraud activities that have returned over \$15.6 billion to the federal government through audit and investigative recoveries.⁵ As active partners with the government in contributing information and data to health care fraud prosecutions, health plans are concerned that it is a missed opportunity for their policyholders and employer purchasers when in some instances they are not included in settlements when the Department of Justice or other enforcement agencies enter into agreements and obtain restitution from providers. This is a missed opportunity for federal and state prosecutors as well. Including the amounts lost by private plans, as well as public programs, in their prosecutions is likely to allow federal and state prosecutors to seek and obtain even larger penalties against those who commit fraud. Recognizing that Medical Supplement insurers, Medicaid health plans, Medicare Advantage plans, and commercial insurers often are adversely affected by health care providers who defraud public programs, health plans should be included in restitution agreements.

Protection for Governmental and Private Plans Working Together

Another issue that deserves scrutiny is whether private health plans may be subject to lawsuits as a result of supplying information on cases of suspected fraud to law enforcement agencies. HIPAA contains only a limited immunity provision⁶ that appears to confer “qualified immunity” for providing information regarding fraud and abuse, but solely to the Secretary or Attorney General. Thus the possibility exists that a health plan might be found civilly or criminally liable for providing what it believes to be accurate information on cases of suspected fraud and abuse to a government agency, even at the government agency’s request. There have been situations where unscrupulous providers have chosen to sue health plans for libel or other charges when under investigation for suspected fraud. A number of states have recognized the chilling effect such lawsuits or threatened actions have on robust private sector initiatives and have enacted limited immunity statutes for health care fraud; all states, as well as the federal government, should do so.

⁵ Testimony of Lewis Morris, Chief Counsel OIG, House Committee on Ways and Means, June 15, 2010.

⁶ 42 U.S.C. § 1320a-7c, 42 U.S.C. § 1320c-6.

To expand and clarify the HIPAA language, we recommend that stronger protections be created by setting up a “safe harbor” for health plans supplying information concerning suspected health care fraud to not just the Secretary or Attorney General, but to any other private or public entity. This should include protection for health plans, should they report suspected health care fraud on any NAIC Uniform Fraud Reporting Form specifically developed for health insurance fraud reporting. Such a safe harbor should apply unless the information is false and the person providing it knew, or had reason to believe, that the information was false.

IV. Conclusion

Thank you for considering our perspectives on the important national goal of preventing and detecting health care fraud and, in so doing, improving health care quality and patient outcomes for the American people. We stand ready to work with the Committee to address opportunities for strengthening fraud prevention in both the private sector and public programs.