U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
OFFICE OF INSPECTOR GENERAL

Testimony Before the United States Senate
Special Committee on Aging

"Protecting Seniors from Identity Theft: Is the Federal Government Doing Enough?"

Testimony of:
Gary Cantrell
Deputy Inspector General for Investigations

Office of Inspector General
Department of Health and Human Services

October 7, 2015
2:00 pm
Location: Dirksen Senate Office Building, Room 562

Testimony of: **Gary Cantrell**
Deputy Inspector General for Investigations
Office of Inspector General, U.S. Department of Health and Human Services

Good afternoon, Chairman Collins, Ranking Member McCaskill, and distinguished members of the Committee. I am Gary Cantrell, Deputy Inspector General for Investigations with the U.S. Department of Health and Human Services (HHS) – Office of Inspector General (OIG). I appreciate the opportunity to appear before you to discuss medical identity theft in Federal health care programs and our efforts to fight this threat.

Our mission at OIG is to protect the integrity of HHS programs as well as the health and welfare of program beneficiaries. A majority of OIG's resources go toward the oversight of Medicare and Medicaid programs that represent a significant part of the Federal budget and that affect this country's most vulnerable citizens. In a given year, the amount of work conducted in each category is set by the purpose limitations in OIG's appropriations.

OIG is a leader in the fight against Medicare fraud. We use data analytics to detect and investigate program fraud and to target our resources for maximum results. Our partnerships with other Government entities and the private sector are also invaluable to our enforcement successes. Medical identity theft represents a growing danger to patients and health care programs, including Medicare and Medicaid. We commend the Committee's efforts to draw much-needed attention to this type of fraud. Today's testimony discusses OIG's enforcement efforts to detect, prevent, and investigate health care fraud involving medical identity theft in Federal health care programs.

OIG IS A LEADER IN THE FIGHT AGAINST MEDICARE FRAUD

OIG advances our mission through a robust program of investigations, audits, evaluations, enforcement actions, and compliance efforts. In today's testimony, I focus on our law enforcement activities, led by my division, the Office of Investigations. We collaborate with our OIG colleagues, which include attorneys, evaluators, auditors, and data analytics experts. The Office of Investigations is the law enforcement component of OIG and investigates fraud and abuse against HHS programs. Our special agents have full law enforcement authority and affect a broad range of actions, including the execution of search warrants and arrests. We use traditional, as well as state-of-the art investigative techniques and innovative data analytics to fulfill our mission.

Our OIG investigations have produced record-setting results. During the last 3 fiscal years (FYs 2013-2015), OIG investigations have resulted in over $10.9 billion in investigative receivables (dollars ordered or agreed to be paid to government programs as a result of

criminal, civil, or administrative judgments or settlements); 2,856 criminal actions; 1,446 civil actions; and 11,343 program exclusions.

The return on investment for our work is significant. OIG, and our HHS and Department of Justice (DOJ) partners, have returned $7.70 for every $1 invested in the Health Care Fraud and Abuse Control Program (HCFAC).[1] HCFAC is OIG's largest funding source. Since HCFAC's inception in 1997, its activities have returned more than $27.8 billion to the Medicare Trust Funds. HCFAC's continued success confirms the soundness of a collaborative approach to identify and prosecute the most egregious instances of health care fraud, to prevent future fraud, and to protect program beneficiaries.

MEDICAL IDENTITY THEFT POSES SERIOUS RISKS TO PATIENTS AND HEALTH CARE PROGRAMS

Medical identity theft is the appropriation or misuse of a patient's or a provider's medical identifying information (such as a Medicare identification number) to fraudulently obtain or bill for medical care, prescription drugs, or supplies. It can affect beneficiaries or providers. Such theft can create patient safety risks and impose financial burdens on those affected. It can lead to erroneous entries in beneficiaries' medical histories and even lead to the wrong medical treatment. Medical identity theft may also lead to significant financial losses for the Medicare Trust Funds and taxpayers.[2] OIG has seen a variety of such fraud, as well as related schemes that go beyond the traditional boundaries of medical identity theft.

Medical identity theft includes the theft of Personally Identifiable Information (PII), such as Social Security numbers, dates of birth, and credit card and bank account information that are highly valued by identity thieves. It may also include Protected Health Information (PHI), such as health history, medical diagnoses, services rendered, or health care billing or payment information. We primarily see the theft of PII in our enforcement work, but whether the information compromised is PII or PHI, the theft of this sensitive information can result in significant financial loss, damaged credit scores, and costly legal problems. Of grave concern is the possibility that someone's PHI could be compromised and result in patient harm because of incorrect information in a personal medical record (either hardcopy or electronic). A false diagnosis, an inaccurate blood type, or even an incorrect medication included or omitted in an official medical record could result in serious patient harm. For the purposes of today's testimony, I will refer to the types of information involved in medical identity theft as sensitive information.

[1] Data from the *Health Care Fraud and Abuse Control Program FY 2014 Report*, available at http://oig.hhs.gov/publications/docs/hcfac/FY2014-hcfac.pdf.
[2] HHS-OIG report: *CMS Response to Breaches and Medical Identity Theft*, October 2012 (OEI-02-10-00040)

MEDICAL IDENTITY THEFT CAN TAKE MANY FORMS

Medical identity theft fraud is perpetrated by a broad range of bad actors – from health care providers to criminal enterprises. Health care providers who commit medical identity theft often rely on a relationship of trust with an unsuspecting patient. Health care providers can include physicians, nurses, pharmacists, ambulance drivers, and medical assistants. Health care providers and other non-provider employees in the health care industry pose a particular challenge because of their often unrestricted access to sensitive information. Also of concern is the number of Medicare and Medicaid beneficiaries who are either tricked into providing sensitive information, or at worst, are co-conspirators in the fraud scheme.

While each medical identity theft case is unique, these cases can generally be categorized into external and internal threats. External threats often include the involvement of con artists and professional identity thieves who target vulnerable seniors and program beneficiaries, often through social engineering. Of concern is the external threat posed by criminal enterprises. Internal threats include health care company owners, employees, physicians, non-physician practitioners, and patients who participate in a fraud scheme. Additional detail regarding these external and internal threats is discussed below.

OIG IS DEDICATED TO FIGHTING HEALTH CARE FRAUD BY CRIMINAL ENTERPRISES, WHICH POSE SIGNIFICANT THREATS TO MEDICARE AND ITS BENEFICIARIES

OIG dedicates significant resources to investigate health care fraud schemes perpetrated by both domestic and transnational organized criminal enterprises. Some transnational criminal enterprises recruit individuals from their countries of origin to execute illicit acts and shield the leaders from direct involvement in the execution of the schemes. Others target individuals from their country of origin as fraud victims because of a high level of trust and strong cultural ties. Health care fraud schemes by transnational criminal enterprises often involve the theft or sale of sensitive information, which is used to defraud Medicare and other health care programs.

We view complex health care fraud schemes perpetrated by criminal enterprises as a priority. These groups take a systematic, organized approach to committing fraud. Criminal enterprises have become a pervasive problem in fraud schemes involving home health, durable medical equipment (DME), prescription drugs, transportation, and medical clinic settings. Criminal enterprises may solicit persons to use as "straw" business owners for a sham corporation, or they may steal physician or other identities to bill Medicare and other health insurance carriers for false claims. They often hire recruiters to buy lists of patient names and identification numbers, or identify parties willing to participate in the fraud schemes. These groups pose a threat to the integrity of HHS programs because their primary

objective is to organize with the intent of stealing as much money from Federal health programs as quickly as possible. Two examples of criminal enterprises involved in medical identity theft schemes are included below.

In one case, a transnational criminal organization established a "ghost" medical clinic using stolen information from a physician in the local area. Members of the conspiracy enrolled the clinic in Medicare, established bank accounts, linked the bank accounts to a fictitious address (a mailbox store), registered the clinic with the Secretary of State, and began to bill Medicare. All together, the "ghost" clinic billed Medicare over $1 million, with Medicare paying about $350,000 worth of claims. The money that was paid was laundered through out-of-state banks and shell businesses by members of the conspiracy. The supervisor of the conspiracy was sentenced to 57 months in prison and others have been indicted.

In another identity theft case, a mastermind was sentenced to 37 months in prison for his involvement in an Armenian-American organized criminal enterprise engaged in a wide range of fraudulent activity, including the operation of a $100 million Medicare billing ring. In this national, multiagency investigation, a large-scale law enforcement operation was conducted that involved the arrest of over 50 individuals in multiple states. At the time, it was the largest Medicare fraud scheme ever perpetrated by a single criminal enterprise and charged by DOJ. According to the indictment, the defendants stole the identities of numerous physicians and thousands of Medicare beneficiaries and operated at least 118 different phony clinics in 25 states for the purposes of submitting Medicare claims for reimbursement.

OIG HAS ALSO UNCOVERED INSIDER THREATS INVOLVING PROVIDER AND PATIENT CO-CONSPIRATORS

Those who work in the health profession could have access to significant amounts of sensitive information. The following examples are illustrative of our work in this area.

In Some Cases, Health Care Company Owners Mastermind Fraud Schemes
Health care company owners are a particular problem in medical identity theft schemes because they may mastermind a fraud scheme without the knowledge of the company employees or patients. In one case, OIG investigated a home health agency owner who paid illegal kickbacks to patient recruiters to obtain the information of Medicare beneficiaries; this information was used to submit over $12 million in false claims to Medicare for home health services that were not medically necessary or never provided. The owner also created fictitious patient files in an attempt to deceive a Medicare auditor and make it appear as though home health services were provided and medically necessary. The defendant was sentenced to 80 months in prison and ordered to pay $14.1 million in restitution.

In another matter, OIG investigated a fraud case in which a hospice owner paid an individual large amounts of money to illegally obtain names and other sensitive information for multiple Medicare beneficiaries. The hospice owner used that illegally obtained beneficiary information to fraudulently bill Medicare for millions of dollars of hospice services that were never provided or were for beneficiaries who were not eligible for those services. The hospice owner was sentenced to 70 months imprisonment and 3 years of supervised release. The individual who sold the sensitive information for illegal use was sentenced to 14 months imprisonment and 3 years of supervised release.

Unscrupulous Health Care Employees Present Fraud Vulnerabilities

Health care company employees present a unique challenge to the problem of medical identity theft because of their knowledge about program vulnerabilities and level of access to sensitive information. In a recent Medicare Fraud Strike Force case, a visiting physician group billed Medicare over $4 million using deceased patient information for home health services. The medical biller, office administrator, and medical director also billed for services that were never provided, using information from former medical professionals without their knowledge. The company's administrator and biller forged physician signatures on medical documents, and directed physicians to create false documentation to support billing for services that were never rendered. The medical biller was sentenced to 45 months in prison for her role in the scheme, while the office administrator was sentenced to more than 7 years in prison. The medical director pleaded guilty and is awaiting sentencing.

Physicians and Other Health Care Providers Have Also Committed Identity Theft and Fraud

Medical identity theft is not limited to health care employees and can include clinicians, such as physicians and nurses. For example, OIG jointly investigated a case in which a physician violated his agreement with the United States to be excluded from all Federal health care programs for 10 years. After his exclusion, the physician developed a sophisticated scheme to defraud Medicare and Medicaid and to continue collecting Federal reimbursement. This scheme involved shell owners, forged signatures, and theft of the identity of another doctor to fraudulently bill Medicare and Medicaid for laboratory services. The physician was convicted of multiple charges related to health care fraud, bankruptcy fraud, filing false tax returns, and aggravated identity theft. He was sentenced to over 8 years in prison and 3 years of supervised release, was fined over $2.6 million and ordered to pay restitution of over $260,000. He was also ordered to forfeit over $1 million.

OIG has investigated numerous cases involving nonphysician health care practitioners who commit medical identity theft. In one case, OIG investigated a pharmacy chain owner who engaged in a health care fraud scheme by submitting false claims for prescription refills. The pharmacy owner billed Medicare and Medicaid for prescription refills when the beneficiaries had not requested refills and indeed did not receive the refills. The medications targeted for these refills were often expensive HIV and cancer medications intended for very

ill customers. The pharmacy owner, along with co-conspirators, falsely used the names and sensitive information of hundreds of beneficiaries to conduct this fraud. The defendant was convicted of health care fraud and aggravated identity theft.

Although Program Beneficiaries Are Typically Victims of Medical Identity Theft, in Some Cases They Are Co-Conspirators

Patient co-conspirators can be a significant problem in medical identity theft schemes by selling their sensitive information (usually their Medicare or Medicaid numbers) to identity thieves for a small kickback. OIG continues to investigate cases in which patients sell their sensitive information and receive medically unnecessary (often sham) services in exchange for a kickback.

One example involving prescription drug fraud involved a physician who wrote illegal prescriptions for complicit beneficiaries, who were transported by the vanload to his practice. There they received medically unnecessary prescriptions for oxycodone-based products. The pseudo-patients provided their Medicare, Medicaid, and private insurance information that was used to pay for the prescriptions, then passed more than 700,000 pills to 6 different drug trafficking organizations. The physician, along with 61 of his associates, received a combined 253 years in prison. The physician himself received 20 years and was ordered to forfeit $10 million.

In one high-profile case, an OIG investigation into a medical clinic unraveled a $20 million fraud scheme in which thousands of anti-psychotic medications were fraudulently prescribed, using stolen Medicare beneficiary identities and recruited homeless veterans. The clinic owner conspired with her mother-in-law to fill the fraudulent prescriptions at various pharmacies. Once the drugs were filled, the clinic purchased the prescriptions from recruited veterans being treated for drug addiction and schizophrenia. After purchasing the drugs from beneficiary co-conspirators, the clinic diverted the drugs to the black market, where they were sold to other pharmacies and rebilled to health care programs. To date, 16 defendants have been convicted for their roles in this scheme. The clinic owner has pleaded guilty to conspiracy to commit health care fraud and identity theft and has been sentenced to 8 years for overseeing the conspiracy.

OIG IS LEVERAGING A RANGE OF OPPORTUNITIES TO COMBAT FRAUD INVOLVING MEDICAL IDENTITY THEFT

Data Analytics Support OIG Fraud Identification and Investigation

OIG is a front-runner in the use of data analytics to detect and investigate health care fraud. We use innovative analytic methods to analyze billions of records and data points to identify trends that may indicate fraud, geographical hot spots, emerging schemes, and individual providers of concern. At the macro level, we analyze data patterns to assess fraud risks

across a spectrum of services and geographic areas to prioritize and deploy our resources. At the micro level, we use data analytics, including near-real-time data, to identify fraud suspects and conduct our investigations efficiently and effectively.

Medicare Fraud Strike Forces Exemplify Enforcement Success

The remarkable success of the Medicare Fraud Strike Force (Strike Force) showcases the effectiveness of our use of data analytics to detect and investigate health care fraud, including schemes that involve medical identity theft. The Strike Force effort began in March 2007, and in 2009 HHS and DOJ announced the formal creation of the Health Care Fraud Prevention and Enforcement Action Team, a joint agency initiative known as HEAT. A key component of HEAT is the Strike Force, which harnesses the efforts of OIG and DOJ, including headquarters, Offices of U.S. Attorneys, and the Federal Bureau of Investigation, along with State and local law enforcement, to fight Medicare fraud in geographic hot spots. The Strike Force teams use near-real-time data to pinpoint fraud hot spots and aberrant billing as it occurs. This coordinated and data-driven approach to identifying, investigating, and prosecuting fraud has produced record-breaking results. Since its inception in March 2007, the Strike Force has charged over 2,300 defendants who collectively have billed the Medicare program over $7 billion.

HEAT actions have led to a 75 percent increase in individuals charged with criminal health care fraud during the initial stages, and the program has maintained significant enforcement success throughout its history. Through HEAT, we have expanded Strike Force teams to operate in nine locations: Miami, Florida; Detroit, Michigan; southern Texas; Los Angeles, California; Tampa, Florida; Brooklyn, New York; southern Louisiana; Chicago, Illinois; and Dallas, Texas.

In a recent example, a national Strike Force operation in June 2015 resulted in charges against 243 individuals, including 46 doctors, nurses, and other licensed medical professionals, for their alleged participation in multiple Medicare and Medicaid fraud schemes involving about $712 million in false billings. The defendants were charged with various health care fraud-related crimes, including conspiracy to commit health care fraud, violations of the anti-kickback statutes, money laundering and aggravated identity theft. The charges were based on a variety of alleged fraud schemes involving various medical treatments and services, including home health care, psychotherapy, physical and occupational therapy, DME, and pharmacy fraud. This coordinated takedown was the largest in Strike Force history, both in terms of the number of defendants charged and loss amount. The cases are currently being investigated and prosecuted by Strike Force teams.

OIG Is Maximizing Its Fraud Fighting Impact Through External Partnerships

In addition to internal collaboration, OIG continuously engages with external stakeholders to enhance the relevance and impact of our work to combat health care fraud, as demonstrated

by our leadership in the Healthcare Fraud Prevention Partnership (HFPP)[3], our association with the National Health Care Anti-Fraud Association (NHCAA), and our support to the Senior Medicare Patrol (SMP).

The HFPP is a groundbreaking partnership between the Federal and private sectors to share data and information for the purposes of detecting and combating fraud, waste, and abuse in health care. The HFPP was created as a voluntary public-private partnership, between the Federal Government, State officials, private health insurance organizations, and health care antifraud associations. The NHCAA is the leading national nonprofit organization focused exclusively on combating health care fraud and abuse.[4] The NHCAA mission is to protect and serve the public interest by increasing awareness and improving the detection, investigation, civil and criminal prosecution, and prevention of health care fraud and abuse. Both organizations are engaged in efforts to combat the problem of medical identity theft.

OIG, through OI, has worked collaboratively with the SMP[5] to combat medical identity theft. In conjunction with the SMP, OI agents conduct regular presentations designed to educate Medicare and Medicaid beneficiaries on the threat of medical identity theft, and how to protect their sensitive information.

Consumer Education Efforts Are a Key Tool for Preventing Fraud

While data-driven efforts and our external partnerships are invaluable to our enforcement successes, we are not focused solely on enforcement. The best way to combat fraud is by preventing it in the first place, and OIG's oversight efforts support all aspects of program integrity. We strive to cultivate a culture of compliance in the industry through various efforts, including education and guidance. Robust oversight of medical identity theft goes beyond enforcement efforts, and the need to educate providers and consumers (those who could be targeted as victims or co-conspirators) is a critical part of the solution.

OIG conducts a wide variety of consumer education efforts, including offering multiple resources on our public web site at http://oig.hhs.gov/fraud/medical-id-theft/. Our resources include a medical identity theft brochure that is available in an easy-to-read printable format and translated into multiple languages. OIG has also made a significant effort to highlight the problem of medical identity theft through media outreach, including through national television appearances on shows, such as *Good Morning America*, and in widely read journals such as the New England Journal of Medicine and publications such as *USA Today* and the *Wall Street Journal*.

[3] For more information on HFPP, visit: http://hfpp.cms.gov/.
[4] For more information on NHCAA, visit: http://www.nhcaa.org/.
[5] For more information on SMP, visit http://www.smpresource.org/.

Removal of SSNs from Medicare Cards Is an Important Step Toward Preventing Medical Identity Theft

Mitigating the problem of medical identity theft requires an "all hands on deck" approach. We want to thank Congress for its effort to prevent medical identity theft. Because of the Members of this Committee and Congress in passing the CHIP Reauthorization Act of 2015, the removal of Social Security numbers from Medicare cards is now underway. This is an important first step in protecting Medicare beneficiaries' sensitive information, and we thank the Members of this Committee for the attention they continue to place on this important issue.

CONCLUSION

OIG is committed to our continuing oversight of HHS programs and protecting them and their beneficiaries from fraud, waste, and abuse. We will continue to leverage our analytic, investigative, and oversight tools, as well as our partnerships within the law enforcement and program integrity communities, to maximize our efforts. We will continue our enforcement efforts to detect, investigate, and prevent medical identity theft in the Federal health care programs, and will remain vigilant to emerging trends, such as the growing threat of cyber breaches affecting our programs.

We would like to express our appreciation to Congress for its sustained commitment toward our mission and appreciate the Committee's interest in the vital issue of protecting Medicare and other HHS programs and their beneficiaries from fraud. This concludes my testimony. I would be happy to answer your questions. Thank you.