November 23, 2011

Medical Identity Theft/Fraud Convictions Show Health Care Providers, Plans & Other Businesses Must Safeguard Health & Other Information, Guard Against Fraud Schemes

A Federal judge sentenced 25 year old Miami resident Yenky Sanchez, 25 to serve more than 5 years in Federal prison for his role in the theft of Medicare numbers and other information of elderly and disabled Florida residents as part of a plan to defraud Medicare, Medicaid and other federal programs. Coming on the heels of a November 3 conviction in West Virginia of Sargis Tadevosyan in a separate identity theft for Medicare fraud scheme, the convictions highlight the growing commitment and effectiveness of Federal and state investigators in investigating and prosecuting individuals who seek to use identity theft schemes to defraud Medicare or other federal programs.

Sanchez Conviction & Sentencing

The sentence arises from criminal charges brought by the U.S. Department of Justice (DOJ) in conjunction with other federal and state agencies, which charged Sanchez considered to commit health care fraud, authentication feature fraud and aggravated identity theft. According to DOJ documents, Sanchez, participated in a scheme with Raul Diaz-Perera, to steal and sell Medicare numbers and other data about clients of their employer, the Florida Department of Children and Families' (DCF). Diaz-Perera previously was employed with DCF.

According to the evidence at trial against Sanchez and a factual proffer filed with the court during the plea hearing for co-defendant Diaz-Perera, Sanchez used his position as employees at a DCF call center in downtown Miami to steal Medicare numbers and other personal information for purposes of committing health care fraud and identity theft.

According to Federal prosecutors, Sanchez used his access as an employee to the DCF internal computer system to obtain the names, addresses, telephone numbers, dates of birth, Social Security numbers, and Medicare numbers of 148 elderly and disabled Floridians who had applied to DCF for food stamps, cash benefits, and Medicaid. Sanchez then gave the personal identification information to Diaz-Perera, who sold it to a third party in October, 2010. The intent was for those numbers to be used to fraudulently bill Medicare for services that were never provided to the DCF beneficiaries.

Prosecutors also claimed that Diaz-Perera again turned to Sanchez and. Sanchez again used his access to the DCF computer system to steal the names and other identification information, including Medicare numbers of more than 400 beneficiaries in January, 2011. Prosecutors charged that Sanchez was to be paid $4.00 for each Medicare number he stole from DCF.

Sanchez was convicted of conspiring to commit health care fraud, in violation of Title 18, United States Code, Section 1349; conspiring to commit authentication feature fraud, in violation of Title 18, United States Code, Sections 1028(a)(3) and (f); and aggravated identity theft, in violation of Title 18, United States Code, Section 1028A(a)(1). Based on these convictions, U.S. District Judge Cecilia M. Altonaga sentenced Sanchez on November 21, 2011 to 65 months in prison, followed by three years of supervised release. Judge Altonaga also imposed a $5,000.00 fine on Sanchez.

Tadevosyan Conviction

Federal officials previously also had scored another Medicare fraud/identity theft prosecution victory just a few short weeks earlier in West Virginia. On November 3, 2011, a federal jury convicted Armenia citizen Sargis Tadevosyan in connection with a health care fraud scheme that intended to defraud millions of dollars from Medicare. Tadevosyan was found guilty of two felony counts: conspiracy to commit health care fraud and wire fraud and aggravated identity theft. Tadevosyan faces up to 20 years in prison for the conspiracy conviction and a mandatory consecutive sentence of two years for aggravated identity theft and a $250,000 fine when he is sentenced on January 26, 2012.

In contrast to the small scale conspiracy that apparently occurred in the Sanchez case, the Tadovosyn scheme apparently was orchestrated by organized crime. Testimony brought forth at trial revealed that in the fall of 2010, an individual known as "Garik" asked co-conspirators Arsen Bedzhanyan, 23 and Igor Shevchuk, 22, to open up bank accounts using names and false identification documents that Garik would provide and told them that the names belonged to real people who had left the United States. The co-conspirators agreed to participate in the scheme in exchange for $5,000 each from "Garik." To further the scheme, "Garik" gave each of the co-conspirators identification documents, which included fake driver's licenses with the names of other individuals. Bedzhanyan and Shevchuk admitted to using the false identification documents to open bank accounts in the names of several false front providers at banks located in and around Charleston.

In April 2011, agents with the Department of Health and Human Resources Office of Inspector General (HHS-OIG) began investigating fraud schemes involving false front providers, whereby a company posed as a Medicare health care provider, and unlawfully billed Medicare as if they were providing legitimate services. After following numerous leads, investigators discovered that false front provider companies: ASC Solutions, Attens Reliable, Inc., KB Support Group, Inc., Powersource Support, Inc., Mega Plus Solutions Corp., were set up to advance the health care fraud scheme in and around Charleston, West Virginia. In total, more than $4 million in Medicare claims were submitted by the false front providers.

Evidence at trial showed that on May 6, 2011, the defendant picked up co-conspirators Shevchuk and Bedzhanyan in New York City and drove them to West Virginia. Evidence also showed that the defendant provided Shevchuk and Bedzhanyan with false identification documents and also dropped his associates off near a United Bank in Dunbar, West Virginia. At the time of the scheme, Shevchuk also used a false driver's license in the name of Klim Baykov, the purported owner of KB Support Group, Inc. and signed documents which enabled him to make changes to the company's bank account. Federal agents subsequently arrested the defendant and his co-conspirators in West Virginia.

Co-conspirators Shevchuk and Bedzhanyan previously pleaded guilty in September to aiding and abetting aggravated identity theft in connection to the health care fraud plot. Both defendants are scheduled to be sentenced on December 1, 2011.

In announcing the Tadevosyan conviction, federal officials affirmed their commitment to finding and prosecuting identity theft targeting Medicare and other health insurance programs. "This investigation revealed that organized criminal groups are still brazenly attempting to steal taxpayer money from our national health insurance programs," said Nicholas DiGiulio, Special Agent in Charge for the Inspector General's Office of the United States Department of Health and Human Services. "Today's results demonstrate that we will do whatever it takes to catch these individuals in the act before they receive a penny of taxpayers' money."

Federal Laws, Investigations & Prosecutions of Medical Identity Theft Schemes Tightening

Whether from deliberate schemes to misappropriate data or other less sinister compromises of personal health information or other sensitive data, health care providers, health plans and other businesses face rising responsibilities to protect data and increasing exposures for failing to do so.

Federal law imposes stiff sanctions against organizations and individuals that engage in theft of personal or other sensitive information, health or other federal program fraud or both. In an effort to stem the tide of health care and identity theft fraud, federal and state legislators and regulators have tightened federal and state laws to strengthen laws prohibiting health care fraud and identity theft, to require that health care providers, health plans, federal and state agencies and others that collect, possess or access sensitive personal health information, personal financial information or other sensitive date safeguard and protect sensitive information against improper access or misuse, to increase the penalties for violation of these federal and state laws and to provide law enforcement with expanded tools to investigate and prosecute violations of these laws. See e.g., **Cybercrime and Identity Theft: Health Information Security Beyond HIPAA.**

As a result of these new and expanded mandates, health care providers, health plans, financial organizations and a broad range of other businesses and governmental agencies face a host of complicated mandates to protect personal health information, personal financial information and other sensitive data under laws such as the Health Information Portability & Accountability Act (HIPAA), the Fair & Accurate Credit Transactions Act (FACTA), state and federal identity theft and data security and other laws. In addition to taking steps to protect sensitive data, these and other organizations often face specific obligations to monitor and report potential data breaches, to train staff and other members of their workforce, and to take other steps to prevent or redress potential breaches or other wrongful use or access of this and other sensitive information. Businesses and agencies subject to these requires may face significant criminal, civil, and/or administrative liability for failing to fulfill these requirements. See e.g., **OCR Audit Program Kickoff Further Heats HIPAA Privacy Risks; UCLA Health Systems Payment of $865,500 To Settle HIPAA Charges Shows Rising HIPAA Risk; CVS Settles Privacy Charges; Rite Aid Agrees to Pay $1 Million to Settle HIPAA Privacy Case As Office of Civil Rights Proposes Tighter HIPAA Privacy & Security Regulations; 2 New HIPAA Criminal Actions Highlight Risks From Wrongful Use/Access of Health Information; President Signs Long-Sought Red Flag Rule Exemption Into Law.**

Health care providers, health insurers and others handling protected health information are particularly at risk when their data is compromised. Recent amendments to HIPAA require these entities and their business associates to tighten their data privacy and security safeguards and to monitor and timely report data breaches, as well as significantly expand their potential liability exposure for failing to comply with HIPAA's requirements. As amended by the American Recovery and Reinvestment Act of 2009 in Section 13411 of the HITECH Act, requires HHS to provide for periodic audits to ensure covered entities and business associates are complying with the HIPAA Privacy and Security Rules and Breach Notification standards. To implement this mandate, OCR is piloting a program to perform up to 150 audits of covered entities to assess privacy and security compliance between November 2011 and December 2012.

As part of its ongoing implementation of stepped up enforcement responsibility and powers enacted as part of these recent amendments, the HHS Office of Civil Rights (OCR) announced on November 8, 2011 its kickoff of a new compliance audit effort. **OCR Audit Program Kickoff Further Heats HIPAA Privacy Risks.**

These developments send a forceful message that all businesses generally and health care providers, health plans, healthcare clearinghouses and their business associates specifically must get serious about compliance with the privacy, security and data breach requirements of HIPAA and other applicable law by implementing and administering the policies, procedures, training and oversight necessary to comply with these and other federal and state mandates regarding the protection of personal health information and other sensitive data.

For Help With Compliance, Investigations Or Other Needs

If you need assistance providing compliance or other training, reviewing or responding to these or other health care related risk management, compliance, enforcement or management concerns, the author of this update, attorney Cynthia Marcotte Stamer, may be able to help. Vice President of the North Texas Health Care Compliance Professionals Association, Past Chair of the ABA Health Law Section Managed Care & Insurance Section and the former Board Compliance Chair of the National Kidney Foundation of

North Texas, Ms. Stamer has more than 24 years experience advising health industry clients about these and other matters. Ms. Stamer has extensive experience advising and assisting health care providers and other health industry clients to establish and administer medical privacy and other compliance and risk management policies, to health care industry investigation, enforcement and other compliance, public policy, regulatory, staffing, and other operations and risk management concerns. A popular lecturer and widely published author on health industry concerns, Ms. Stamer continuously advises health industry clients about compliance and internal controls, workforce and medical staff performance, quality, governance, reimbursement, and other risk management and operational matters. Ms. Stamer also publishes and speaks extensively on health and managed care industry regulatory, staffing and human resources, compensation and benefits, technology, public policy, reimbursement and other operations and risk management concerns/ She also regularly designs and presents risk management, compliance and other training for health care providers, professional associations and others. Her publications and insights appear in the Health Care Compliance Association, Atlantic Information Service, Bureau of National Affairs, World At Work, The Wall Street Journal, Business Insurance, the Dallas Morning News, Modern Health Care, Managed Healthcare, Health Leaders, and a many other national and local publications. You can get more information about her health industry experience **here**. If you need assistance with these or other compliance concerns, wish to inquire about arranging for compliance audit or training, or need legal representation on other matters please contact Ms. Stamer at (469) 767-8872 or via e-mail **here**.

Other Recent Updates & Information

If you find this of interest, you also be interested reviewing some of our other articles and publications by Ms. Stamer including:

- **Detroit-Area Foot Doctor Pleads Guilty to Medicare Fraud Scheme**
- **Merck To Pay $950 Million To Settle Vioxx® Off-Label Marketing Charges**
- **Texas Medical Board Suspends Child Psychiatrist For Sexual Misconduct**
- **100,000+ Primary Care Providers Signed Up To Get EHRs Regional Extension Centers**
- **Joint Commission Equal Visitation Rules & Guidance Supplement New Medicare Equal Visitation Requirements**
- **OCR Audit Program Kickoff Further Heats HIPAA Privacy Risks**
- **Houston Doctor Gets 135 Month Health Care Fraud Sentence**
- **Bill Extending Funding For Certain Veteran Medical and Other Projects Heads To President**
- **OCR Settlements Show Health Care & Disabled Housing Providers Face Growing Disability Discrimination Risks**
- **UCLA Health Systems Payment of $865,500 To Settle HIPAA Charges Shows Rising HIPAA Risk**
- **Indictment of 91 Shows Growing Health Care Fraud**
- **Unions Get New Tool As NLRB Changes Bargaining Units Certification Rules For Non-Acute Health Care Facilities**
- **Texas Doctor, Pharmacy Suspension Reminder of Pain Management Prescribing Risks**
- **Supreme Court Ruling Medical Resident Stipend Are Wages Highlights Advisability of Compliance Review**
- **Minimum Wage, Overtime Risks Highlighted By Labor Department Strike Force Targeting Residential Care & Group Homes**
- **DEA Cautions Practitioners Must Restrict Delegation of Controlled Substance Prescribing Functions, Urges Adoption of Written Policies & Agreements**

You can review other selected publications and resources and additional information about the employment, employee benefits and other experience of Ms. Stamer **here.**

If you or someone else you know would like to receive future updates about developments on these and other concerns, please be sure that we have your current contact information – including your preferred e-mail – by creating or updating your profile **here**. For important information concerning this communication click **here.** If you do not wish to receive these updates in the future, send an e-mail with the word "Remove" in the Subject to **here.**