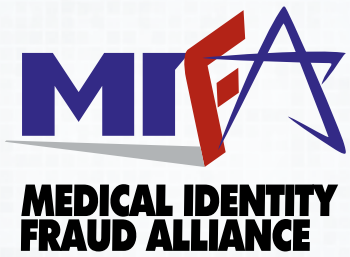

The Growing Threat of Medical Identity Fraud: A Call to Action

A Publication of The Medical Identity Fraud Alliance

July 2013

Visit us at www.MedIDFraud.org

MEDICAL IDENTITY FRAUD ALLIANCE

ABOUT THE MEDICAL IDENTITY FRAUD ALLIANCE (MIFA)

MIFA is the first public/private sector-coordinated effort with a focused agenda that unites all the stakeholders to jointly develop solutions and best practices for fighting medical identity fraud. The Alliance is dedicated to helping its members better protect consumers from medical identity theft and the resulting financial, physical, and emotional damage it can cause. Together, we aim to increase awareness through education, while promoting best-in-class technologies and practices and influencing government regulations, policies, and laws. Specifically we:

- **Mobilize** the healthcare ecosystem.
- **Cooperate** to leverage collective power.
- **Research** to adequately understand the problem.
- **Educate** consumers, industry, legislators, and regulators.
- **Empower** individuals to be the first line of defense in safeguarding their Protected Health Information (PHI)

Author

Gary R. Gordon, Ed.D.
Bluewater International

Contributors

Christine Arevalo
ID Experts

Deanna L. Jones
ID Experts

Rick Kam
ID Experts

Jack Price, CFE, ALHC, AHFI
Medical Identity Fraud Alliance (MIFA)

Robin Slade
Medical Identity Fraud Alliance (MIFA)
Foundation for Payments Fraud Abatement & Activism (FPF2A)
The Santa Fe Group

Norman A. Willox, Jr.
Bluewater International

Visit us at www.MedIDFraud.org

MEDICAL IDENTITY FRAUD ALLIANCE

INTRODUCTION

Ten years ago, very few professionals or consumers knew anything about financial identity theft and fraud; today it is general knowledge. Likewise, today very few professionals or consumers are aware of medical identity theft and fraud and its potential for harm. Policy decision-makers, organizations that hold protected health information (PHI), law enforcement, regulatory agencies, and consumer advocates now have an opportunity and obligation to bring this serious societal problem to the forefront and work together to protect the public.

The use of another person's PHI to gain medical services, to procure drugs, or to defraud private insurers or government benefit programs, such as Medicare and Medicaid, is pervasive and threatens the health of individuals and the trust in the healthcare system, and also contributes significantly to the rising cost of healthcare. The threats to individuals include contamination of their health records with erroneous information including, among others items, blood type, serious health conditions, and prescription drugs. Fraud losses in the healthcare system are astronomical and in most cases are facilitated by a stolen medical identity of an individual or a provider.

For the purposes of this paper, medical identity fraud is defined as *the fraudulent use of an individual's protected health information (PHI) and personally identifiable information (e.g, name, Social Security number) to obtain medical goods and service or to gain financial benefit.*[1] *Medical identity theft is defined as the stealing of an individual's protected health information PHI.*

PHI is accessible in many places today, unlike when paper records were the norm. While improving the sharing of information in the healthcare systems, the transformation to electronic health records (EHR) has made patient records more vulnerable to data breaches. The EHRs are found on mobile devices (laptops, smartphones, tablets) throughout the healthcare organization (covered entity), as well as shared with an organization's business associates--companies that help the covered entity carry out its healthcare functions.

There are a number of contributing factors that, when taken as a whole, demand immediate action by all stakeholders in the healthcare ecosystem. These include the electronic pervasiveness of PHI and the required security measures required to protect it, the changing regulatory landscape, the increased number of individuals with healthcare benefits, more alternative delivery models with care provided outside of facilities, the increased value of PHI to criminal organizations and the rapidly escalating sophistication of domestic and international crime organizations.

1 Synthetic or fictitious identities have been used to commit medical identity fraud too. In this situation, criminals combine pieces of personal identifier information and protected health information from several individuals to create a blended identity.

MEDICAL IDENTITY FRAUD ALLIANCE

UNDERSTANDING THE THREAT OF MEDICAL IDENTITY THEFT AND FRAUD

Few people think of themselves as having a medical identity and thus the idea of someone stealing their medical identity is not even on their radar screen. For example, if you ask someone what steps they would take to reduce the chance of identity theft if they lost their wallet, they would tell you that they would cancel their credit cards, contact their bank if they have a debit card and apply for a new driver's license. Rarely, would they mention alerting their health insurance company to take measures equivalent to canceling a credit card. What the public does not yet realize is its medical identities have a significant street value and that a nefarious individual can easily gain access to medical services through the use of their stolen medical identity, the result of which can cause them great harm.

The consequences of medical identity fraud can be more complex than that of the greater known financial identity fraud. Financial losses, inability to purchase a house or car, and not being approved for a loan are all consequences that are easily understood if your good credit is comprised by your financial identity being stolen. It is easy to understand why criminals would want to steal an individual's financial identity, as they can profit from using the information in a number of ways.

The consequences of medical identity theft are only evident when an individual seeks and is denied legitimate services, is denied health insurance, receives unnecessary or inaccurate healthcare (sometimes life threatening), is turned down for a job based on an inaccurate health condition, and/or receives notification from a collection agency of a bill that was not received and is past due. These events occur less frequently than the number of credit card transactions most people have in a month. However, the likelihood of a life threatening event and the average financial loss per incident makes this a much more insidious act.

The two anecdotal real life examples presented here illustrate the challenges that victims of medical identity fraud face.

EXAMPLE 1

John Doe was in the U.S. Army Reserve and had been called to active duty. When he went to Iraq with his unit, he left his medical insurance card issued through his employer at home for safekeeping.

John had a brother, Joe, who was chronically unemployed, a drug abuser, and in poor health. Joe was driving under the influence, had a horrible accident, and was airlifted to the region's best trauma center. Joe used John's insurance card. After several hundred thousand dollars of medical treatment, it came to light that Joe was not John. John's medical history was corrupted by Joe's medical history of drug abuse and the accident.

MEDICAL IDENTITY FRAUD ALLIANCE

EXAMPLE 1 (CONTINUED)

About the time John returned from Iraq, the fraud was discovered and John was almost terminated by his employer. An investigation revealed the true facts and that John had never been aware of what was done to steal his identity. He was an innocent victim. The hospital that provided the treatment agreed to reimburse the employer's insurance company for all payments and filed a civil action against Joe to collect their losses. It took John over a year to correct his medical records.

EXAMPLE 2

An elderly gentleman went to his local ER for a back injury. While receiving treatment, the doctor on call noticed he also had an infection in a lymph node, which could easily be treated with antibiotics. Based on the chart and medical history, the doctor announced he would administer a course of penicillin. The gentleman vehemently objected and immediately asked the doctor why he thought that would be an appropriate antibiotic, as it should be clear from his medical records that he has a life-threatening allergy to penicillin. The doctor reviewed the notes thoroughly. After verifying the information, the doctor shared that he had simply followed the same methods administered for the gentleman's "last visit" to the ER when he had not only been prescribed penicillin but a bevy of additional medications to which he had no allergic reactions. This was the gentleman's first ever visit to the small town ER.

EXAMPLE 2 (CONTINUED)

At that point, both the doctor and the patient realized something was wrong. Further research revealed that someone had used his medical insurance ID card to obtain services at that very hospital. The gentleman admitted later that he had lost his medical insurance ID card a few months prior and had just recently received his replacement card in the mail. He also said he hadn't thought much of it because he "didn't think it was a big deal."

He now treats his medical insurance card with the same security he does his Social Security card. He doesn't like to talk about this ordeal because he could have died from a single injection of penicillin.

SIZE, SCOPE, AND TRENDS OF MEDICAL IDENTITY THEFT AND FRAUD

What is known about the size and scope of medical identity theft is a result of studies utilizing self-reported survey methodology and anecdotal cases. These studies provide insight into the problem and some trending analysis, but little information on the perpetrators or their modus operandi.

The following findings are from three annual studies conducted from 2010–2012 by the Ponemon Institute.[2]

The studies indicate the number of medical identity theft victims in the United States is increasing. In 2010, the estimated number of victims was 1.42 million. It increased in 2011 to 1.49 million and to 1.85 million in 2012.

Seventy five percent of the survey respondents who were victims of medical identity theft reported financial consequences. Half of them made out of pocket payments to their health plan or insurer to restore their coverage. Approximately 20% of the respondents stated that they had a diminished credit score as a result of the experience. "Lost time and productivity trying to fix inaccuracies in credit report" impacted 20% of the respondents. Of those surveyed, 15% incurred legal costs and 7-8% experienced an increase in their health premiums. About a quarter of the respondents did not experience any financial consequences.

Many respondents indicated that there were non-financial consequences as a result of being victimized. The impact on their healthcare benefits and their treatment were the most egregious. In 2011, 49% of the respondents' health insurance policies were terminated. In 2012, it was 41%. "Mistreatment of an illness because of inaccuracies in health record" was reported by 18% in 2011 and 14% in 2012. In the same two studies, "misdiagnosis of illness because of inaccuracies in health record" was a factor in 10% and 12% of the cases, respectively. The 2012 study reported that 51% of the victims lost trust and confidence in their healthcare provider as a result of being a victim of medical identity theft.

The consensus of experts is that the value of medical identities is greater than Social Security numbers on the black market. A recent investigative reporter interviewed a medical identity theft middleman who confirmed this perception.[3] Some estimates suggest that criminals are monetizing medical identities at a rate that is between 20 and 50 times more than financial identities. "A stolen medical identity has a $50 street value--whereas a stolen Social Security number, on the other hand, only sells for $1," said Kirk Herath, Nationwide Chief Privacy Officer. "However, while most people are very careful with their Social Security number to protect their credit and personal information, they tend to be less careful when it comes to their medical information."[4]

Given the value of PHI on the black market, criminals will continue to buy large sets of breached PHI data and exploit the vulnerabilities that exist in systems and devices that store PHI. The higher street value of PHI will only increase the number of victims of medical identity theft.

2 Ponemon Institute, First Annual National Survey on Medical Identity Theft, February, 2010: Ponemon Institute, Second Annual Survey on Medical Identity Theft, March 2011: Ponemon Institute, Third Annual Survey on Medical Identity Theft, June, 2012.

3 Your Medical Records Could be Sold on the Black Market, NBC Bay Area News, http://www.nbcbayarea.com/investigations/Medical-Records-Could-Be-Sold-on-Black-Market-212040241.html, June 19, 2013.

4 http://www.nationwide.com/newsroom/061312-MedicalIDTheft.jsp.

The FBI reports that healthcare fraud costs the United States at least $80 billion a year and is rising.[5] Given that most healthcare fraud requires a medical identity or a provider identity, any reduction in medical identity theft will have a significant impact on provider fraud and other types of healthcare fraud.

THE INDIVIDUAL MUST BE THE FIRST LINE OF DEFENSE

While there are many solutions that attempt to detect medical fraud, the amount of fraud continues to increase. Borrowing again from the lessons learned in other industries, there is a need to engage with the healthcare plan member in order to detect the fraud scheme as early as possible. The credit card industry first developed sophisticated analytics and began sharing fraud data to stop credit card fraud. While that was an essential component of the equation, it did not work alone. When the credit card companies began calling customers about transactions flagged by the analytics, the issue of credit card fraud became a reality for the public and consumers became partners in identifying and reducing fraudulent transactions.

Complicated and hard to read Explanations of Benefits (EOBs) are the closest the healthcare industry has come to engaging the consumer. For the most part, individuals receive an EOB for each medical claim for themselves or their dependents. Paper EOBs are mailed to the individual, often 30 days after a service is provided. It is well documented that few people review them, are often unable to decipher the information, and usually are only concerned with the amount they owe.

If they owe nothing, they do not think about checking to see if the claims are for services that they or their dependents received. There is limited evidence of individuals reporting claims that appear to be suspicious to their health plan. EOBs are costly and health insurers have not been successful in communicating their importance to the insured.

It is no wonder that the fraud losses in the healthcare industry are so high and continue to rise. The lack of corroboration from the one source who knows whether they received the medical services handicaps the insurance plan's capability to identity a fraudulent claim in a timely manner. This, coupled with the practice of paying claims quickly and chasing after ones that are later identified as fraud, makes the private or government plans easy targets for bad actors. Sophisticated back-end analytics identify fraudulent trends and patterns too late in the process to prevent questionable claims from being paid. While these methodologies allow for shutting down criminal groups intent on defrauding the system, by the time they do that, the losses have reached a significant level.

The only way to detect fraudulent claims at an early stage is to engage members at the beginning of the claims process. There are major challenges to doing this. Currently, most of the public is unaware of the threat of medical identity fraud, both in terms of their health and the cost.

5 FBI website, http://www.fbi.gov/about-us/investigate/white_collar/health-care-fraud, April 25, 2013.

Assuming public awareness can be raised, the insurers still must convince their members to act. In addition, the issues of security, privacy, and trust will have to be addressed for any solution to be widely accepted.

The earlier credit card industry example provides an understanding of why consumers were willing to participate in efforts to curtail fraud. There were perceived consequences, including identity theft, cancellation of the credit card, the inconvenience of waiting to receive a new one, and the potential liability of an out-of-pocket cost of $50.

Incorporating the consumer as a near real-time authority on the card transaction immediately determined if third party fraud was occurring. This interaction stopped the fraudulent transaction, eliminated the loss, and curtailed further harm. The change in suspect verification workflow substantially reduced credit card fraud in the United States. It should be noted the consumer greatly appreciated the engagement by the financial institution and saw it as a consumer benefit, which helped grow the customer base for the credit card company.

RECOMMENDED ACTIONS

Leadership: Establish Public-Private Partnerships

There needs to be a coordinated approach to address medical identity fraud, as individual stakeholders cannot solve this societal problem alone. Fortunately, there have been several efforts that provide a foundation from which to address this issue. The World Privacy Forum has been a leader in raising awareness.[6]

The federal government has focused attention through studies, such as the one commissioned in May 2008 by the Office of the National Coordinator for Health Information Technology. [7]

What is required next is a public-private sector partnership to bring together the key stakeholders and provide a cohesive approach to the problem. It must include the private sector component of the healthcare ecosystem, which up to now has had a limited response to the medical identity problem.

The Medical Identity Fraud Alliance (MIFA) was recently formed to address the issues raised in this paper. MIFA is comprised of key stakeholders from the healthcare industry, security, compliance, and privacy companies, government, law enforcement, nonprofit organizations, and academe. MIFA will provide leadership to:

- Develop an awareness, education, and training campaign for the public and the healthcare industry.
- Inform public policy decision makers about medical identity theft and fraud and its current and evolving impact through awareness, education, and research programs.
- Establish a comprehensive applied research agenda.

6 Pam Dixon, Medical Identity Theft: The Information than can kill you, Spring 2006.

7 Booz Allen Hamilton, Medical Identity Theft Final Report, January 2009.

- Promote and encourage innovative best practices, processes, and technology to prevent and detect medical identity theft and fraud.

Public-private partnerships have historically been successful in solving societal problems that cannot be resolved by a single stakeholder, be it government, law enforcement, the private sector, non-profit organizations, or academe. Leaders from each of these stakeholder groups must join together and be willing to share information and resources for the partnership to succeed.

AWARENESS, EDUCATION, AND TRAINING CAMPAIGN

Closing the gap in the public's awareness is the first step in combating medical identity fraud. Fortunately, the identity theft awareness campaign of the past ten years provides an excellent roadmap. A concerted effort by government organizations, including the Federal Trade Commission (FTC), Department of Justice (DOJ), coupled with consumer groups, and the financial service industry, have made the public cognizant of the threats posed by identity theft and procedures to mitigate it. A similar campaign must be initiated to raise the awareness of medical identity theft and fraud.

In addition to the public, this awareness campaign must reach healthcare payers and providers, law enforcement, public policy decision makers, and non-profit organizations that have considerable contact with consumers concerning health insurance. While many of the personnel from these entities have some appreciation for medical identity fraud, it is not being addressed. For example, in interviews with directors of several health insurance company Special Investigation Units (SIU), they stated that they have not focused specifically on these cases, nor have they searched their data for medical identity fraud.[8] Law enforcement organizations that investigate healthcare fraud are focusing their resources on provider fraud. As with the identity theft education campaign, public policy decision-makers will need to be educated if legislation and regulation are going to play a part in solving this societal issue. Raising the awareness of medical identity fraud and the consequences of it is only the first step. Training programs will need to be developed for the personnel of insurance plans and providers, as well as for the law enforcement community.

APPLIED RESEARCH AGENDA

A literature review indicates that there is a limited but growing body of knowledge on medical identity theft and fraud, with most of it performed through survey research. This research provides some insight into the level of awareness of medical identity theft, victimization rates, and anecdotal cases that illustrate how the crime is committed.

A collaborative applied research effort, with the necessary multi-disciplinary talent, resources, data sources, and analytical capabilities are needed to drive innovation and inform policy decision makers.

8 Phone interviews conducted by Rick Kam and Gary Gordon, March 2012.

This research should employ several methodologies and provide results to:

- Measure and understand the size and scope of medical identity theft and fraud, including causes and trends.
- Identify the changing threats from insiders and criminal organizations.
- Determine the impact of data breaches and cyber attacks.
- Determine best practices for authentication, data security, and privacy protection technologies and methods.
- Determine effective policy and regulatory decisions.

After identifying the academic, government, commercial, and non-profit groups currently conducting research on medical identity theft and fraud, identity theft, and other related areas, MIFA will convene a meeting of these stakeholders with the goal of developing a comprehensive research agenda and a plan to fund it.

INNOVATIVE NEW SOLUTIONS

New products and services need to be developed (or existing products and services adapted) for protecting an individual's medical identity, for early detection of medical identity fraud, and enhanced security of PHI data. These solutions must:

- Provide a means for an individual to monitor, validate, and verify the claims against his/her medical identity in near real time.
- Provide new analytics that detect anomalies early in the processing of a claim.
- Provide better authentication of the identities of individuals requesting healthcare services.
- Provide for greater security and privacy of an individual's healthcare records as they are transmitted throughout the healthcare ecosystem.
- Provide a means for victims of a PHI breach to monitor and protect their medical identities.

Adopting and adapting successful best practices from other sectors will allow for rapid impact and benefits, while reducing critical damage, harm, and liability.

PUBLIC POLICY, LAW, AND REGULATION

A document compiling current laws, both federal and state, and relevant regulatory statutes and guidance must be created. This document will provide the basis for the following:

- A review of current laws and regulation to identify where gaps exist.
- A public policy research agenda to determine the effectiveness of current solutions or to understand the impact of potential public policy initiatives.

- Discussion topics for key stakeholders to address at workshops, symposia, and conferences.
- Identification of areas that require solutions to close gaps.
- Enhancement of the Consumer Bill of Rights to encompass healthcare and its unique ecosystem and regulatory environment.

CALL TO ACTION

The key stakeholders must take this opportunity to tackle the emerging threat of medical identity fraud. Dissemination of information that quickly educates and raises the awareness level must be undertaken. Technologies and services that allow for medical identity monitoring, increased identity authentication, and threat identification must be developed and made widely available.

The recommendations stated in this white paper provide a blueprint for controlling medical identity theft and fraud before the number of victims reaches epidemic proportions. By forming MIFA several key stakeholders have begun this process. They cannot do it alone. New levels of cooperation and information sharing are required.

ABOUT THE AUTHOR & CONTRIBUTORS

Gary R. Gordon, Ed.D., Managing Partner
Bluewater International

Dr. Gordon is a leading security expert and thought leader and has developed innovative educational programs and training, cutting-edge applied research to understand critical societal problems, and been the executive director of three public-private partnerships. He has authored several white papers on identity fraud and was the principal investigator for a Bureau of Justice Assistance funded project: Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement. Released in October 2007, this empirically based study of closed U.S. Secret Service cases from 2000-2006, provides insight into offender characteristics, the crimes, and the victims.

Christine Arevalo, Director of Healthcare Identity Management
ID Experts

Christine Arevalo is a founding employee of ID Experts. She has experience managing risk assessments, complex crisis communication strategies, and data breach response for healthcare organizations. Christine actively drives industry initiatives on healthcare identity management and has contributed to national discussions on how to prevent, detect, and remediate medical identity theft.

MEDICAL IDENTITY FRAUD ALLIANCE

Deanna L. Jones, CFE, Investigations Unit Manager
ID Experts

Deanna Jones heads the ID Experts' Special Investigations Unit and came to IDE from the field of law enforcement. She has an extensive background in legal and insurance investigations, as well as identity fraud and medical identity theft investigation. Deanna is a Certified Fraud Examiner with government security clearance.

Rick Kam, President
ID Experts

Rick Kam is an expert in the area of privacy and information security. He has extensive experience leading organizations in the development of policy and solutions to address the growing problem of protecting PHI/PII and remediating privacy incidents and identity theft.

Jack Price, CFE, ALHC, AHFI, Development Coordinator
Medical Identity Fraud Alliance (MIFA)

Jack is a Development Coordinator for the Medical Identity Fraud Alliance and has an extensive history in security and fraud reduction. Jack, a former law enforcement officer and executive in the insurance industry, recently retired from BlueCross BlueShield of Tennessee where he served as Chief Security Officer. He is a former president of International Claim Association (ICA), and former Chairman for the National Health Care Anti-Fraud Association (NHCAA).

Robin Slade, Development Coordinator
Medical Identity Fraud Alliance (MIFA), Foundation for Payments Fraud Abatement & Activism (FPF2A), The Santa Fe Group

Robin is a Development Coordinator for the Medical Identity Fraud Alliance and has spent the last decade as a leader in helping financial services executives develop fraud risk management best practices and tactical solutions. Robin launched FPF2A and FraudAvengers.org, a non-profit corporation founded in 2010, to identify, understand, and resolve the root causes of payments fraud. Robin is the Chief Operating Officer and Senior Vice President for The Santa Fe Group and The Shared Assessments Program.

Norman A. Willox, Jr., Managing Partner
Bluewater International

Norm Willox is the Chief Executive Officer and Founder of Bluewater International, with significant experience developing high growth companies within a variety of sectors, including Insurance, Financial Services, Energy, Healthcare, Government, Law Enforcement, Cyber Security and Homeland Security. Norm founded Bluewater as a way to seek out and support select "for profit" companies that focus on solving critical social risk issues with a business model that is reoccurring and sustainable, and thus having a lasting positive and societal impact.