The World Privacy Forum

First report in a series

MEDICAL IDENTITY THEFT: The Information Crime that Can Kill You

Spring 2006

Pam Dixon
World Privacy Forum
May 3, 2006

Brief Summary of Report

This report discusses the issue of medical identity theft and outlines how it can cause great harm to its victims. The report finds that one of the significant harms a victim may experience is a false entry made to his or her medical history due to the activities of an imposter. Erroneous information in health files can lead and has led to a number of negative consequences for victims. Victims do not have the same recourse and help for recovery from medical identity theft as do victims of financial identity theft. This report analyzes statistics in health care and identity theft, and estimates that approximately a quarter million to a half million individuals have been victims of this crime. The report presents the specific harms of medical identity theft based on analysis of cases, and explains why the falsification of information in victims' medical files is one of the crime's core harms. The report reviews the planned National Health Information Network and why the network may facilitate this crime. The report explains the reasons why medical identity theft is challenging to detect, and discusses the specific ways consumers have discovered they were victims of this crime.

Summary of Findings and Recommendations

This report finds that medical identity theft is deeply entrenched in the health care system. Identity theft may be done by criminals, doctors, nurses, hospital employees, and increasingly, by highly sophisticated crime rings. The report finds that medical identity theft victims need an expanded right to correct their medical files in order to recover from this crime, and need more specialized consumer education that is focused on correcting the specific harms of medical identity theft. Key recommendations in the report include:

- Individuals' rights to correct errors in their medical histories and files need to be expanded to allow them to remove false information from their files.
- Individuals should have the right to receive one free copy of their medical file.
- Individuals should have expanded rights to obtain an accounting of disclosures of health information.
- Studies are needed to determine what the incidence of medical identity theft is, how and where it is occurring, and how it can be detected and prevented.
- Notification of medical data breaches to consumers has the potential to save lives, protect health, and prevent losses.
- All working prototypes for the National Health Information Network need comprehensive risk assessments focused on preventing medical identity theft while protecting patient privacy.

About the World Privacy Forum

The World Privacy Forum is a non-profit public interest research and consumer education group. It focuses on a range of privacy matters, including financial, medical, employment, and Internet privacy. The World Privacy Forum was founded in 2003.

Index

BRIEF SUMMARY OF REPORT 2

SUMMARY OF FINDINGS AND RECOMMENDATIONS 2

ABOUT THE WORLD PRIVACY FORUM 2

INDEX 3

PART I: SUMMARY 5

THE DANGEROUS IMPACT OF MEDICAL IDENTITY THEFT 5
MEDICAL IDENTITY THEFT, THE CRIME THAT HAS HIDDEN ITSELF ALL TOO WELL 8
THE VICTIMS' PERSPECTIVE: LACK OF RECOURSE, LACK OF RIGHTS, AND LACK OF HELP 8
ELECTRONIC RECORDS, HEALTH NETWORKS, AND THE CHALLENGES MEDICAL IDENTITY THEFT BRINGS TO BOTH 9
MEDICAL IDENTITY THEFT VICTIMS ARE FALLING THROUGH GAPS 10
BACKGROUND OF THIS REPORT 11
FINDINGS 12
RECOMMENDATIONS 15

PART II: DISCUSSION 16

DEFINITION OF MEDICAL IDENTITY THEFT 16

FRAUD OR IDENTITY THEFT? 17
UNDERLYING THINKING: WHAT MEDICAL IDENTITY THEFT IS NOT 18

MEDICAL IDENTITY THEFT BY THE NUMBERS: HOW PREVALENT IS THIS PROBLEM? 19

STATISTICS SPECIFIC TO MEDICAL IDENTITY THEFT 20
Federal Trade Commission Medical Identity Theft Complaints 20
Social Security Administration/Office of Inspector General (SSA/OIG) Hotline Data 21
FTC 2003 Identity Theft Survey 21
Identity Theft Resource Center 2003 and 2004 Survey 21
Number of Prosecutions 22
Conclusions regarding the medical identity theft indicators 22
BACKGROUND: GENERAL STATISTICS ON IDENTITY THEFT 23
BACKGROUND: GENERAL STATISTICS ON HEALTH CARE FRAUD 24
Hotline Statistics 25
Referrals the Inspector General's Office of HHS took Some Form of Action On 25

THE HUMAN COST OF MEDICAL IDENTITY THEFT 26

FINANCIAL LOSSES 28
HARM FROM FALSE ENTRIES PUT IN MEDICAL RECORD 28
DENIAL OF INSURANCE, INSURANCE CAPS REACHED 29
LOSS OF REPUTATION: 29
Physician Loss of Reputation: Theft of Physicians' Identities 30
LOSS OF MEDICAL RECORD PRIVACY: SUBPOENAS 30
LOSS OF TIME 30

HOW PEOPLE HAVE DISCOVERED THEY ARE VICTIMS OF MEDICAL IDENTITY THEFT 30

COLLECTION NOTICES 31

Receipt of Someone Else's Bills 32
Notification by Law Enforcement or an Insurance Company 33
Notification by a Health Care Provider 33
Medical Problem at an Emergency Room 33
Notification of Data Breach by a Medical Provider 34
Denial of Insurance Coverage, Notification that Benefits have Run Out, or "lifetime cap" Has Been Reached 34
Review of Explanation of Medical Benefits Notices 35

SOME DYNAMICS OF MEDICAL IDENTITY THEFT 35

Falsification of Medical Charts is a Root Issue 35
Who Commits Medical Identity Theft? 36
Organized Crime *37*
Solo Identity Thieves *37*
Doctors and Other Health Care Providers *38*
Relatives of beneficiaries *38*
Opportunists *38*
Medical Identity Theft is a Crime that Hides 38

RECOURSE AND RECOVERY ISSUES FOR VICTIMS 39

Financial Recovery Tools are Available for Victims 39
Correcting and Recovering from the Medical and Insurance Aspects of Medical Identity Theft is Difficult 40
Why Can't Victims Correct Their Medical Records? 40

MEDICAL IDENTITY THEFT AND HIPAA 42

HIPAA and Accounting for Disclosures 42

THE SECURITY ISSUES THIS CRIME RAISES 44

Data Breaches and Medical Identity Theft 44
New Polling Methods for Post-Breach Studies are Needed *45*
Data Breach Notification Needs to go to Each Individual Impacted *44*
The National Health Information Network and Medical Identity Theft 45
The Lessons the NHIN Needs to Learn from the High Incidence of Fraud in Medicare / Medicaid Electronic Systems *46*
Current Audit Systems Do not Resolve The Problem 47
Digital Security Issues in the NHIN and Other Highly Digitized, Virtualized Environments 48
Physical Security Issues in a Medical Environment 49

WHAT'S NEXT? GOING FORWARD FROM HERE 51

The Necessity of a Comprehensive Risk Assessment 51
Legitimate Drug Trials and Medical Researchers Need to Differentiate Themselves From Fraudsters 51
Further Study: Getting a Grasp of the Size, Scope, Incidence of This Problem is Crucial 53

NEW CONSUMER TIPS FOR MEDICAL IDENTITY THEFT VICTIMS 53

CONCLUSION 54

CREDITS 55

REPORT AUTHOR: 55

FOR MORE INFORMATION: 56

MEDICAL IDENTITY THEFT: The information crime that can kill you

Part I: Summary

Medical identity theft is a crime that can cause great harm to its victims. Yet despite the profound risk it carries, it is the least studied and most poorly documented of the cluster of identity theft crimes.[1] It is also the most difficult to fix after the fact, because victims have limited rights and recourses. Medical identity theft typically leaves a trail of falsified information in medical records that can plague victims' medical and financial lives for years.

Medical identity theft occurs when someone uses a person's name and sometimes other parts of their identity – such as insurance information -- without the person's knowledge or consent to obtain medical services or goods, or uses the person's identity information to make false claims for medical services or goods. Medical identity theft frequently results in erroneous entries being put into existing medical records, and can involve the creation of fictitious medical records in the victim's name.

As the health care system transitions from paper-based to electronic, this crime may become easier to commit. Victims may find it more difficult to recover from medical identity theft as medical errors are disseminated and redisseminated through computer networks and other medical information-sharing pathways. The time has come for substantive attention to and understanding of this crime.

The Dangerous Impact of Medical Identity Theft

Victims of medical identity theft may experience the now-familiar consequences of financially oriented forms of identity theft. These can include the loss of credit, harassment by debt collectors, and inability to find employment. Recently, a Colorado man whose Social Security Number, name, and address was stolen, found out he was a victim of medical identity theft when a bill collector wrote to demand the $44,000 he owed to a hospital … for a surgery he never had. The victim did not have insurance, and had to go through a lengthy procedure to clear his name, a process that is ongoing after more than two years.[2]

---

[1] For a description of identity theft crimes and statistics about the incidence of these crimes, see Federal Trade Commission, Identity Theft Survey Report (Sept. 2003). The complete report is available at: <http://www.consumer.gov/idtheft/pdf/synovatereport.pdf>.

[2] Littleton Police Department, Inclusive Case Report, March 25, 2004 (Case 2004001789).

But unlike purely financial forms of identity theft, medical identity theft may also harm its victims by creating false entries in their health records at hospitals, doctors' offices, pharmacies, and insurance companies. Sometimes the changes are put in files intentionally; sometimes the changes are secondary consequences of the theft. The changes made to victims' medical files and histories can remain for years, and may not ever be corrected or even discovered.

Victims of medical identity theft may receive the wrong medical treatment, find their health insurance exhausted, and could become uninsurable for both life and health insurance coverage. They may fail physical exams for employment due to the presence of diseases in their health record that do not belong to them. It is nightmarish that patients' medical records may include information about individuals who have stolen their identities for the purposes of using the victims' insurance or for dodging medical bills. However, evidence exists that this is already occurring.

- A Boston area psychiatrist made false entries in charts of individuals who were not his patients. He gave individuals diagnoses of drug addiction and abuse, severe depression and numerous psychiatric sessions which they did not actually have, then used their personal information to submit false bills to insurance. The victims, after learning of the crime, had difficulties getting the false information removed from their medical files. One woman told an investigator that she "is concerned about obtaining future health insurance coverage … because her husband is self-employed."[3]

- Another non-patient of the same Boston psychiatrist discovered that his medical record had been falsified to include numerous psychiatric sessions that did not occur and false diagnoses of severe depression.[4] He discovered the false diagnoses after he had applied for employment.

- One medical identity theft victim from Florida went for medical treatment and says she found that her medical files had been altered. She said that she discovered that an imposter had caused false entries on her file, including changes to her blood type.[5]

- An Ohio woman, while working at a dental office, accessed protected patient information and used the information to phone in prescriptions to area pharmacies. According to the Office of Inspector General, Health and Human Service, she "called in prescriptions in her name as well as the names of Medicaid recipients."[6]

---

[3] United States v. Skodnek, 933 F. Supp. 1108,; 1996 U.S. Dist. LEXIS 9788 (D. D. Mass. 1996).
[4] *Ibid.*
[5] Comment of L. Weaver in Federal Trade Commission, Identity Theft Victim Assistance Workshop,(Aug. 18, 2000), <http://www.ftc.gov/bcp/workshops/idtheft/comments/weaverlind.htm>
[6] Office of Inspector General, Health and Human Service, Criminal Actions (Sept. 2005), <http://oig.hhs.gov/fraud/enforcement/criminal/05/0905.html>.

- In another case, a Missouri identity thief used multiple victims' information to establish false drivers' licenses in their names. The thief entered a regional health center, acquired the health record of the victim she was impersonating at the time, and intentionally altered the records in order to obtain a prescription in the victim's name.[7]

- A Pennsylvania man discovered that an imposter used his identity at five different hospitals to receive more than $100,000 worth of medical treatment. At each hospital, the imposter created medical histories in the victim's name.[8]

- Victims in Southern California were given medical tests by non-physicians and had false diagnoses inserted into their medical files by a sophisticated, organized network of medical imaging companies. The individuals, according to an indictment, actively recruited Medicare beneficiaries with the promise of free transportation, food, and medical care. The perpetrators, posing as doctors and health professionals, obtained the victim's personal information and photocopied the victim's Medicare cards. The operation raked in $909,000 using victims' personal and insurance information. [9]

Medical identity theft is not as well known as financial identity theft yet. Some of its victims have certainly taken note of it, as have some health care providers. Some providers at Kaiser Permanente, a health network with 30 medical centers and 431 medical offices, now ask to see a driver's license in addition to the program's health card.[10] The University of Connecticut Health Center, concerned after a case of medical identity theft occurred there, began checking patient driver's licenses. Staff at the health center told researchers that approximately a dozen people each week attempted to impersonate beneficiaries. Health center staff was concerned about the health dangers of false entries in medical records arising from medical identity theft. [11]

New York Attorney General Eliot Spitzer specifically discussed medical records and medical privacy issues and gave advice about protection of these records in 2005 identity theft education materials.[12] Some insurers have begun mitigation efforts by educating their beneficiaries about the problem. Blue Cross/Blue Shield's web site, for example, warns about identity theft in the medical context. Its site advises consumers that identity

---

[7].United States v. Sample, 213 F. 3d 1029, 2000 U.S. App. Lexis 11945. (8th Cir. 2000).
[8] United States v. Sullivan, Affidavit of Probable Cause for Arrest Warrant. Also see "AG Corbett announces arrest of Philadelphia man in $144,000 identity theft scam," Press Release, July 29, 2005. Available at <http://www.attorneygeneral.gov/press.aspx?id=122>.
[9] United States v. Dzugha, Case No. 5:05-cr-00589-JF, Indictment at 4-7 (N. Cal).
[10] For example, some doctor's offices in the Kaiser Permanente system in San Diego have had signs posted explaining that they ask for ID. < http://www.kaiserpermanente.org/>.
[11] Interviews with hospital staff members. See also University of Connecticut Advance, "Steps taken to stem healthcare identity theft," (Sept.7, 2005), <http://www.advance.uconn.edu/2005/050907/05090711.htm>.
[12] The booklet, "Tips for Protecting Your Privacy: Don't Become a Victim of Identity Theft," April 2005, is available at <http://www.oag.state.ny.us/consumer/tips/identity_theft_pamphlet.pdf>.

theft "using another person's health insurance card or identification to obtain health care or other services or to impersonate that individual,[13] is now among commonly seen scams.

Medical Identity Theft, the Crime That has Hidden Itself All Too Well

Medical identity theft can be difficult to uncover. It is typically well-hidden in large electronic payment systems and in widely dispersed databases and medical files. Medical identity theft does not always reveal itself through traditional financial avenues. Individuals who regularly check their credit reports, for example, may see no indication on the credit report that the problem exists, even if it is a significant one.

The people who commit medical identity theft can be sophisticated professionals who are adept at making sure victims do not detect the crime -- ever. Victims may only discover it many years later through an unhappy circumstance such as the discovery of an incorrect blood type on a medical chart, or the loss of a job opportunity after a background check reveals one or more diagnoses and diseases that didn't belong to them.

Because of the difficulty of detection, the potential exists for this crime to be happening substantially more frequently than anyone has documented to date.

The Victims' Perspective: Lack of Recourse, Lack of Rights, and Lack of Help

Financial difficulties and medical errors introduced into victims' files because of this crime are bad enough. But those who learn that they are victims of medical identity theft have yet another discovery waiting for them: medical identity theft often leaves its victims without substantive recourse or clear pathways to follow for help. Recovery for victims of medical identity may be difficult or impossible because of the lack of enforceable rights, and because of the dispersed and often hidden nature of medical records.

Victims of financial identity theft can depend on rights such as the ability to see and correct errors in their credit report, the ability to file fraud alerts, the right to obtain documents or information relating to transactions involving their personal information, and the right to prevent consumer reporting agencies (such as credit bureaus) from reporting information that has resulted from of identity theft.[14]

But victims of medical identity theft do not have a similar complete set of rights or

---

[13] See <http://www.bcbs.com/antifraud>.

[14] The FTC has a detailed page describing these rights and specific actions to take: Take Charge: Fighting Back Against Identity Theft. <http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm>. See also Government Accountability Office, , Identity Theft Rights: Some Outreach Efforts to Promote Awareness of New Consumer Rights are Underway, (June 2005) (GAO-05-710).

redresses. Victims of medical identity theft do not have the blanket right to correct errors in their medical files. In some cases, victims have not been allowed to even see the compromised files. And victims of medical identity theft do not have the right to prevent health care providers, medical clearinghouses, or insurers from reporting and re-reporting information that has resulted from identity theft.

Medical identity theft victims do not have an easy way to discover who, if anyone, to call for help. Because of how this crime is committed, in some situations, the same people victims may call for help may be among those perpetrating the crime.[15] The mechanisms of this crime mean that victims have a more complex and uncharted path to recovery. Because of this, the advice that is often given to victims of financial identity theft needs to be augmented with specific recommendations for victims of medical identity theft.[16]

Electronic Records, Health Networks, and the Challenges Medical Identity Theft Brings to Both

Further complicating the challenges of medical identity theft is the push to make patient medical records electronic and place patient information in a National Health Information Network (NHIN).[17] Pilot projects to develop four different NHIN prototypes are already underway in at least 12 cities.[18] The digitizing of health records in general and the national network is a process related to an overall transition from paper records to electronic records.

Currently, the mantra is that digitization of patient records will improve health care, reduce fraud, reduce medical errors, and save lives. But this does not account for the challenging reality of medical identity theft and the substantial problems it can introduce into such a system. Many other questions and problems with medical information networks also remain unexplored. While a transition from a paper system to an electronic system is inevitable, the transition must be done correctly and with an acknowledgement of risks such as those medical identity introduces, in mind. Digitized patient records and the National Health Information Network in particular create two significant problems in

---

[15] For example, this situation may occur if the person who stole a victim's identity was impersonating a doctor or working in a clinic. Also see statement of Louis J. Freeh, director, Federal Bureau of Investigation, before the Special Committee on Aging, U.S. Senate. Federal News Service, March 21, 1995.

[16] Beyond resolving the financial impacts of the crime, medical identity theft victims may also need to take action to amend their medical files. One way consumers may be able to pro-actively detect this crime is to request copies of all insurance payments, services, and goods delivered in their name. If a consumer is a victim of this crime, they may not be receiving these explanation of benefit notices.

[17] The National Health Information Network (NHIN) is an ambitious modernization plan proposed by the U.S. government. The idea is to move from paper medical files to electronic medical files that are shared. The government goal is to digitize patients' health records and medical files and create a national network to place the information in. The network, called the NHIN, would be a sophisticated network that hospitals, insurers, doctors, and others could potentially access. For more, see the World Privacy Forum NHIN page at < http://www.worldprivacyforum.org/medicalprivacy_NHIN.html>.

[18] See Astara March, "National health IT system taking off," United Press International, November 10, 2005.

the context of medical identity theft.

- First, the National Health Information Network may make individuals more vulnerable to medical identity theft by making personally identifiable health information more accessible to criminals who have already learned how to work inside the health care system. [19] Digitized information is much more portable and lends itself to rapid transmission. These are usually seen as benefits. But in the hands of an identity thief, these benefits may become liabilities.

- Second, the National Health Information Network as currently conceived may perpetuate and transmit medical errors in ways that have potentially negative consequences. Errors in medical charts and documents arising from medical identity theft could, if left uncorrected as they are by and large today, percolate through a nationwide system. Without more attention, patients who have incorrect files in one city will find their same incorrect files available to all doctors and insurers that use the health network. The same errors may also affect the factual accuracy and quality of medical research and public health interventions based on that data.

The implementation of new technologies in health care need not be a negative development for patient privacy and security. Conversely, neither is the implementation of new technologies a solution that will automatically resolve all problems with medical identity theft. This is especially true when the nature and scope of medical identity theft have not been rigorously studied or acknowledged as a problem. The digitization and wider availability of patient health records without adequate understanding and risk assessment could pose many difficulties.

Medical Identity Theft Victims are Falling Through Gaps

Today, victims of medical identity theft are falling through several existing gaps in consumer and medical arenas. The medical world seldom focuses on financial identity theft, with few knowing the complexities of how to help victims with error reporting problems and so on. Financial identity theft experts are seldom experts in the federal health privacy rule known as HIPAA[20] or in the complexities of the medical care

[19] See statement of Louis J. Freeh, director, Federal Bureau of Investigation, before the Special Committee on Aging, U.S. Senate. Federal News Service, March 21, 1995. From his testimony: "Schemes crafted by health care criminals have changed dramatically in the past few years. Indeed, organized criminal enterprises have penetrated virtually every legitimate segment of the health care industry." Also see Malcolm K. Sparrow, License to Steal: How Fraud Bleeds America's Health Care System, at Introduction and pages 39-52 (Westview Press, 2000).

[20] The Federal health privacy rule was issued by the Department of Health and Human Service under authority granted by the Health Insurance Portability and Accountability Act of 1996. The privacy rules were first issued in 2000 and became effective in 2003. There are also HIPAA rules for security. More information and copies of all the HHS rules and publications can be found at the website of the Office of Civil Rights, which is the HHS agency responsible for enforcement of the HIPAA privacy rule. <http://www.hhs.gov/ocr/hipaa/>.

treatment and payment systems. The Federal Trade Commission (FTC), which has studied financial identity theft, is not responsible for addressing medical issues. That falls to the Department of Health and Human Services, which has not published focused studies or guidance about medical identity theft in particular. The HHS Office of Inspector General investigates cases of generalized health care fraud and abuse, which may only touch the issue tangentially. Statistics on health care fraud are plentiful, but they are not currently sufficient to document the incidence of medical identity theft.

These gaps, which to date have been inadvertent and unintentional, must be closed. Close attention must be paid to the problem of medical identity theft and its victims by Federal and State governments, by private insurers, by researchers, by consumer groups, by patients-rights groups, law enforcement, and other stakeholders who can help create a body of factual knowledge, a pathway of clear, meaningful and effective recourse, and prevention and detection techniques.

Medical identity theft victims need clearer pathways of recourse. The laws that were intended to protect patient medical privacy need to be updated to reflect the reality of medical identity theft. These same laws need to be strengthened to give patients the broader rights they need to correct their medical files, wherever those files may be. Rights that patients currently have under the law to see who has accessed their medical files must be maintained and expanded.

Background of This Report

This report presents information the World Privacy Forum could factually substantiate about medical identity theft, and discusses the reasons why it is essential that this crime be better documented, quantified, and understood.

It is remarkable that medical identity theft has not been recognized as a separate and distinct crime. Despite the lack of comprehensive statistics, it is nonetheless possible to assess the prevalence of medical identity theft by looking more intensively at two crimes of which it is a subset: health care fraud and identity theft.

The World Privacy Forum gathered the information for this report from four primary sources:

- Interviews: The World Privacy Forum interviewed stakeholders, case workers, victims, members of law enforcement, insurers, hospitals and other health care providers, fraud units, prosecutors, HIPAA experts, identity theft experts, fraud experts, health care fraud experts in academia, and others. The goal was to get a "trench-level" view of this subject.

- Prosecutions: A selection of cases of medical identity theft that have come to light through civil or criminal prosecutions were analyzed for this report.

- Three bodies of statistics were reviewed for this report: statistics regarding medical identity theft as found through hotline and survey data, general health care fraud, and general statistics regarding identity theft. Fraud within government health care systems has been studied at length, creating a robust statistical literature, including reports on Medicare/Medicaid fraud and other health care fraud from the Department of Defense, HHS Office of Inspector General, and the Government Accountability Office (GAO). Identity theft material reviewed for this report includes publications from government agencies, in particular the FTC, as well as the GAO and privately issued reports from Javelin and others.

- The World Privacy Forum submitted Freedom of Information Act requests for information at government agencies to acquire relevant information. Some of these requests are still pending, and this report may be updated from time to time as new information becomes available.

Finally, a literature review was conducted looking for reports and studies by relevant associations such as the National Health Care Anti-Fraud Association and others. In some cases, interviews with report authors or the associations were conducted.

A thorough effort was made to uncover relevant material, but this report does not claim to be exhaustive.

Findings

- The World Privacy Forum has found unambiguous substantiation for the presence of medical identity theft as a separate and distinct crime from other forms of identity theft.

- In the cases the World Privacy Forum has analyzed, medical identity theft is a serious information crime that has had substantial consequences on patient well-being, often affects the accuracy of patient medical records, and can impact victims' finances. The crime also entails financial losses to insurers and health care providers. While these losses can be large, the focus of this investigation has been on the effects on individuals.

- There have been 19,428 complaints regarding medical identity theft to the Federal Trade Commission since January 1, 1992, the earliest date the FTC began recording such complaints.

    - Data from government identity theft hotlines and from identity theft surveys containing questions about medical use of data point with some consistency toward a range of approximately 1.5 to 2 percent for the rate of medically-related identity theft in comparison with other forms of identity theft.

- Medical identity theft, as articulated by these numbers, translates in number of victims in 2003 to a range of a minimum of about 3,500 victims to up to a theoretical maximum of almost 3.25 million victims. However, our best estimate is that there could be as many as a quarter to a half million people who have been victims of this crime. [21]

- This crime is under-researched and under-documented. It is probable that more cases exist.

- False entries in medical records are a hallmark of medical identity theft. Victims have had their medical records altered without their permission, consent, and often knowledge. False entries can range from small ones to substantial changes that may introduce medical errors that could be threatening to patient health. Numerous harms to victims can result from false entries in medical records and files.

- False entries made to medical files can be difficult for many victims to find unless they have been notified through some other "crime flag" such as a bill for services they did not receive, or a collections notice from a hospital.

- Victims do not have clear pathways for recourse and recovery. The Fair Credit Reporting Act allows for greater recourse for victims of financial identity theft than the HIPAA health privacy rule provides for victims of medical identity theft. For example, victims do not have the legal right to demand correction of their medical information that was not created by the provider or insurer currently maintaining or using the information. This circularity can make it impossible for a medical identity theft victim to erase false entries from a medical or insurance record. This is true even when false entries were put in the record during the commission of a crime, such as health care fraud or medical identity theft.

- Available evidence suggests that medical identity theft is a crime that is not self-revealing, and is challenging for the average victim to uncover.

- All levels of the medical system may be involved in medical identity theft. Doctors, clinics, billing specialists, nurses, and other members of the medical profession

---

[21] Statistics are from the FTC Identity Theft Clearinghouse data, taken from the FTC Consumer Sentinel database. The bottom range of this figure represents 1.8 percent of 214, 905 victims, which is the percent of victims that said they experienced medical identity theft in 2003. The larger figure of "approximately 3.25 million" is taken directly from the FTC 2003 Identity Theft Survey. The number represents the entire category of "New Accounts & Other Frauds' ID Theft" which includes use of identity information for medical purposes. See pages 4, 13, and Table 1. 2003 FTC Identity Theft Survey Report, September 2003, Federal Trade Commission. "1.5 percent of survey participants reported that in the last year they had discovered that their personal information had been misused to open new credit accounts, take out new loans, or engage in other types of fraud, such as misuse of the victim's name and identifying information when someone is charged with a crime, when renting an apartment, or when obtaining medical care ("'New Accounts & Other Frauds' ID Theft"). This result suggests that almost 3.25 million Americans discovered that their personal information had been misused in this kind of fraud in the past year," p.4. The complete report is available at < http://www.consumer.gov/idtheft/pdf/synovatereport.pdf>.

have taken part in this crime, as have criminals who work in administrative positions inside the health care system to collect information and to carry out their crimes.

- A physician can be the victim of identity theft in the physician's professional capacity. This type of identity theft is often the starting point for propagating incorrect information about patients, and it is often seen when professional crime rings are involved. Thieves can steal a doctor's name, license number, forge a signature, falsify patient records, and forge prescriptions. The problems that health care providers encounter when their professional identities are stolen is beyond the scope of this report.

- Notification of medical data breaches to consumers has the potential to save lives, and protect health.

- Typical studies of data breach victims may not detect medical identity theft, because these studies cannot typically examine changes in the medical files of victims. Victims of medical identity theft may, but do not always have, fraudulent activity noted in their credit reports.

- The circulation of uncorrected errors in digital and paper medical systems may have long-range negative impacts on the viability and accuracy of medical research conducted using patient medical records. This includes medical records from hospitals and from government and state-run programs.

- In at least two documented cases of medical identity theft, hospitals are alleged to have refused to give victims copies of their own health records, or the health records recorded under their name and Social Security Number.

- The proposed National Health Information Network may increase risks to patient safety, privacy, and the security of patient data. There is no indication at this time that the network is being constructed with a specific acknowledgement of medical identity theft.

- An analysis of cases reveals that victims who discover that they are the subject of medical identity theft learn about it in several primary ways: through a collection notice sent to them or in some cases found on a credit report, receipt of someone else's bill, notification by law enforcement or an insurance company, denial of insurance coverage or notification that insurance has reached lifetime caps, or irregularities seen on explanations of medical benefit notices. Less common discovery methods included being notified by a health care provider and noticing discrepancies in the file during medical treatment.

Recommendations

- The issue of medical identity theft needs immediate, thoughtful attention by a range of agencies and bodies, both public and private. It must be studied, quantified, and it must be accurately and vigorously taken into account in public and private systems in a meaningful way.

- Patients need expanded rights to obtain an accounting of disclosures of health information.[22] Expanded maintenance of disclosure histories is essential to tracking the flow of incorrect and fraudulent information inserted into medical files by criminals. The Office of Civil Rights at the Department of Health and Human Services should review the HIPAA health privacy rule and propose changes to expand the rights of medical identity theft victims.

- Patients must have the right to correct and delete errors in their medical record arising from fraud and medical identity theft. All iterations of a patient record must be able to be found and corrected. If this issue is not resolved, patient health and medical research can suffer as a result. The Office of Civil Rights at the Department of Health and Human Services should amend the HIPAA health privacy rule to expand patient rights to amend health records.

- A clear and effective pathway of recourse needs to be developed for victims of medical identity theft that is at least equal to the protections that victims of financial identity theft have. The Office of Civil Rights at the Department of Health and Human Services should work together with the Federal Trade Commission, State Attorneys General, and identity theft victims' organizations to identify and implement solutions for victims.

- Health insurers should send each beneficiary a free annual listing of all claims that were paid and to whom. One of the few effective means of proactively discovering improper use of personal information is for consumers to contact their insurers and ask for a report of all claims paid to their accounts. In this way, patients can learn of changed billing addresses, changed phone numbers, and phony charges that they may otherwise not have seen or noticed.

- Patients should be given the right to receive one free copy of their health record from their health care providers. A 2006 American Health Information Management Association survey found that sixty-three percent of health care providers polled charge patients for copies of their health information. Charges can be up to $5 per page. [23]

---

[22] The accounting of disclosures requirement in the HIPAA health privacy rule requires covered entities to maintain a history of some disclosures of patient information. It also allows patients in some circumstances to obtain a copy of the accounting. 45 C.F.R. § 164.528.

[23] American Health Information Management Association, "The State of HIPAA Privacy and Security Compliance",at 16. Available at <http://www.ahima.org/emerging_issues/2006StateofHIPAACompliance.pdf>.

- Notification to patients is crucial for any data breach that involves patient names and insurance numbers, and the notification should be given promptly. Sometimes the only indication that a medical inaccuracy exists in a file may be found as a result of the database breach notice. Post breach-studies of medical database breaches may have not been configured in a way that will actually find the incidences of medical identity theft, as they do not usually have access to victims' actual medical files.

- The next comprehensive risk assessment of federal computer systems and computer networks with health information should expressly recognize medical identity theft as a specific threat and should determine the risk level of those threats and corresponding vulnerabilities.

- NHIN prototypes, as they become available for testing, need formal risk assessments for medical identity theft. Given the insider nature of this crime, any digitization of medical files in electronic health records and any proposed NHIN needs to be built with an understanding that some doctors, nurses, clinics, and hospitals – as well as their administrative staffs -- may be the bad actors. This poses significant security hurdles, but if these issues are not taken into account now, then the NHIN and other electronic systems can become a means to potentially perpetuate medical errors across the county and facilitate medical identity theft.

Part II: Discussion

Definition of Medical Identity Theft

Medical identity theft occurs when someone uses a person's name and sometimes other parts of their identity – such as insurance information or Social Security Number-- without the victim's knowledge or consent to obtain medical services or goods, or when someone uses the person's identity to obtain money by falsifying claims for medical services and falsifying medical records to support those claims.

Medical identity theft is an information crime and a health crime that can have medical, financial, and other impacts. In this crime, a victim's medical identity is stolen or appropriated in some way. Victims' financial life may be impacted, and there may be other complicating factors. However, the essence of this crime is the use of a *medical* identity by a criminal, and the lack of knowledge by the victim. Medical identities are readily found in medical files and insurance records. Electronic versions of medical

identities appear in electronic health records [24] (EHRs) or large databases, but the essence is the same: in medical identity theft, a victims' medical identity is compromised.[25]

Medical identity theft is a crime that has many operational models. For the purposes of separating medical identity from the plethora of health care fraud and identity theft crimes, this report considers one of the essential hallmarks of medical identity theft to be the use of identity information that results in the falsification of the victims' medical charts with information related directly to the crime, not the actual conditions the real patient has.

Medical identity theft can be seen as a subset of health care fraud. But it is not just that, because the crime can also have financial and other life-consequences. Medical identity theft therefore also needs to be understood in its context as an information crime, that is, as a crime involving theft or abuse of identity information, and as a crime that makes individuals victims in addition to the providers and insurers who may directly bear financial losses.

Operationally, based on known cases, a single thief can steal one or more identities. A doctor can steal patients' identities, as can a clinic or other health provider. It is not unusual in medical identity theft to find cases where entire crime rings purchase hundreds of patient names and insurance information then alter medical files and diagnoses to make millions of dollars in a few months, then move on to new victims.

Medical identity theft can be detected, but typically not by traditional reporting methods associated with financial identity theft. For example, victims may never have their credit cards or credit score affected by this crime. But they may be turned down for jobs, and may potentially have serious medical complications from the crime. For example, victims who have erroneous information put into their health record due to an imposter's activity in their name could receive improper treatment if the errors go undetected by the victim.

Fraud or Identity Theft?

In the identity theft literature, there is a debate over what parts of the crime are "identity *fraud*," and what parts are "identity *theft*."[26] There is not currently a consensus on this definitional issue, and this lack of clarity has impacted a number of survey instruments that quantify identity theft. For example, some do not include credit card fraud in the definition of identity theft. Others do. What most people can agree on is that when a

---

[24] Electronic Health Record (EHR) is one of many terms that describe digitized patient medical and health records. Another term is Electronic Medical Record (EMR.) This report is using the term Electronic Health Record (EHR).

[25] Medical identity theft as the World Privacy Forum is defining it should not be confused with *financial* identity theft that occurs in a medical setting. See the section: "Underlying Thinking: What Identity Theft is Not" in this report.

[26] An identity theft literature review may be found at <http://www.ncjrs.org>. Type in the search term "identity theft" at the site's search box.

person takes over the identity information of another and uses it without consent, that can be called identity theft.

In health care fraud, definitions are even more controversial because of the complexity of those crimes. Numerous kinds of health care fraud exist, and this report does not propose to delve into the deep definitional issues in that field. [27]

This report is a first attempt to define this subset of health care fraud and identity theft. As statistics become available, definitions may sharpen and we may gain a better understanding of the crime.

Underlying Thinking: What Medical Identity Theft is Not

It is important to discuss an underlying aspect of this report's definition of medical identity theft, and that is what is intentionally left out. The following types of health care fraud and identity theft cases were not considered as part of medical identity theft:

- *Some health care fraud cases involve the alteration of patient information, but are not medical identity theft*. For example, a doctor who wants to cover up a medical error may alter patient charts. This is not medical identity theft. The hypothetical doctor falsified records, but did not take over or abuse the identity information of the patient, although the doctor surely abused the patient.

- *Some identity theft cases occur in medical settings, but are not medical identity theft*. For example, if a hospital worker steals patient credit cards or other financially-related identity information and goes on a shopping spree at a mall, that is not medical identity theft but more traditional financial identity theft. In this situation, the medical identity of the person was not impacted, even though their financial information was used.

A razor-thin line exists between some cases of health care fraud. This narrow line can be seen in comparing the following two cases.

- In the case where numerous victims in Southern California were allegedly given medical tests by non-physicians and had false diagnoses inserted into their medical files by a sophisticated, organized network of medical imaging companies, the individuals actively recruited Medicare beneficiaries with the promise of free transportation, food, and medical care. The alleged perpetrators, posing as doctors and health professionals, obtained the victim's personal information and photocopied the victim's Medicare cards. [28] In this case, the victims' information was taken, and the victims did not know their

[27] A definitive review of health care fraud issues may be found in Malcolm K. Sparrow, License to Steal: How Fraud Bleeds America's Health Care System (Westview Press, 2000)..
[28] United States v. Dzugha, No. 5:05-cr-00589-JF, Indictment at 4–7 (N. Cal).

information was going to be used for further billing for visits they never made. The lack of knowledge and consent here is the key point.

Compare the previous case with another case:

- A licensed cardiologist operated on patients, allegedly giving them invasive heart procedures they did not need, for example, angioplasties. Two patients died as a result of the invasive operations. In this case, this was not identity theft, because the patients knew they were being operated on, and a real physician was operating on them. These victims may have been victims of health care fraud and malpractice, but they did not experience medical identity theft as defined in this report. [29]

Medical Identity Theft by the Numbers: How Prevalent is This Problem?

There are unambiguous indications that medical identity exists, and clear indications that this crime is a substantial problem based on the presence of statistical frequency, the presence of prosecutions, and anecdotal evidence from investigators in the field and other members of law enforcement. Statistically, medical identity theft can be viewed both as a subset of identity theft, and as a subset of health care fraud. These two information areas can help gauge the broad trend lines of medical identity theft.

The broad statistics relating to health care fraud clarify that it is an area of crime that rakes in billions of dollars each year. While not all of health care fraud is medical identity theft, the fact that high dollar criminal schemes are already established in this area is not a positive indicator for the chances of medical identity theft going away any time soon. In testimony about the problems of health care fraud FBI director Louis Freeh has said:

> "In South Florida and Southern California, we have seen cocaine distributors switch from drug dealing to health care fraud schemes. The reason - the risks of being caught and imprisoned are less. Drug dealers who are committing health care fraud know that they likely will face only minor punishments because law enforcement is not yet equipped with the laws needed to effectively attack this problem."[30]

The statistics of health care fraud are not currently configured in such a way to allow even an educated guess as to what percent of health care fraud is comprised by medical identity theft. However, general identity theft surveys have included questions about

[29] United States v. Bainbridge Management, No. 1:01 cr 0049, Superseding Indictment (N.D. Ill).
[30] Statement of Louis J. Freeh, director, Federal Bureau of Investigation, before the Special Committee on Aging, U.S. Senate. Federal News Service, March 21, 1995.

medical identity theft, and as such, give more indication as to what percent of identity crimes are comprised by medical identity theft.

The following discussion of the available statistical numbers following looks first at statistics that specifically inform about medical identity theft. A background discussion of overall identity theft statistics and overall health care fraud statistics is included at the end of this section.

Statistics Specific to Medical Identity Theft

There is a small set of statistics that points to medical identity theft. These statistics, when analyzed in conjunction with the larger universe of health care fraud statistics, suggest that medical identity theft, while reported, is likely to be underreported, and that what is seen may be barely the tip of the iceberg.

Consider these numbers:

Federal Trade Commission Medical Identity Theft Complaints

The Federal Trade Commission has recorded that a total of **19,428** individuals have filed complaints specifically concerning medical identity theft at the Federal Trade Commission from January 1, 1992 to April 12, 2006 though its Consumer Sentinel database.[31] For the FTC, which is an agency that does not handle medical issues, nineteen thousand-plus complaints is a high number.

The Federal Trade Commission tracks identity theft complaints through its Identity Theft Clearinghouse. There are two relevant statistics that come from this data: complaints made about use of identity for medical services, and complaints about use of Government benefits, such as Medicare/Medicaid (though this complaint area is not limited to just Medicare/Medicaid.) [32]

- The number of total people identifying themselves as victims of identity theft has risen each year from **86,168** victims in 2001 to **255,565** victims in 2005.

- The number of people who had their Government benefits misused each has risen steadily from **.4** percent of all victims in 2001 to **1.5** percent of all victims in 2005.

[31] Statistic provided in response to a World Privacy Forum FOIA request to the Federal Trade Commission, FTC FOIA-2006-00560.
[32] See the Federal Trade Commission's ID Theft Clearinghouse Data, available at: <http://www.consumer.gov/idtheft/id_federal.htm>.

- The number of people who experienced medical identity theft rose from **1.6** percent in 2001 to **1.8** percent in 2005.

Social Security Administration/Office of Inspector General (SSA/OIG) Hotline Data

The Social Security Administration/Office of Inspector General (SSA/OIG) has a hotline that receives allegation of Social Security Number misuse. A GAO report captured intriguing statistics regarding this hotline. In February 2001, SSA/OIG began sorting their calls into 16 categories of SSN misuse. One of those categories is misuse of Social Security Numbers for medical care. March through September 2001, the fraud hotline received **25,991** identity theft allegations. Medical care comprised **2.1** percent, or **548** allegations.[33]

FTC 2003 Identity Theft Survey

The FTC 2003 Identity Theft Survey identified a broad segment of individuals, who when surveyed said that they had "discovered that their personal information had been misused to open new accounts, to obtain new loans, or to commit theft, fraud, or other crimes. ("New Accounts & Other Frauds" ID Theft)."[34] This group comprised **1.5** percent of all identity theft victims., or almost **3.25** million individuals, according to the FTC. The FTC includes gaining medical treatment in this category. This number indicates that an unknown portion of approximately **3.25** million American adults had their information used to get medical care .

Regarding existing accounts, the FTC found that **2** percent of victims had had their insurance accounts taken over. Again, the type of insurance was not differentiated to be either auto or medical, so this statistic is not highly articulated regarding medical identity theft.

Identity Theft Resource Center 2003 and 2004 Survey

---

[33] Government Accountability Office, Identity Theft Prevalence and Cost Appear to be Growing, March 2002 (GAO-02-363) at 30.

[34] FTC Identity Theft Survey 2003, September 2003. Available at <http://www.consumer.gov/idtheft/pdf/synovate_report.pdf>. See page 4 and page 33. From page 4: "1.5 percent of survey participants reported that in the last year they had discovered that their personal information had been misused to open new credit accounts, take out new loans, or engage in other types of fraud, such as misuse of the victim's name and identifying information when someone is charged with a crime, when renting an apartment, or when obtaining medical care ("'New Accounts & Other Frauds' ID Theft"). This result suggests that almost 3.25 million Americans discovered that their personal information had been misused in this kind of fraud in the past year."

The Identity Theft Resource Center, in its 2003 survey "Identity Theft: The Aftermath 2003" found that 13 percent of respondents said that: "Using my information, someone obtained medical services." The 2004 follow up survey found that 12 victims, or 23 percent of respondents experienced this. Both surveys also found that despite the right to correct records for financial identity theft victims, 70 in 2004 and 66% in 2003 said that there was still negative information in their records.[35] 197 respondents completed the 2004 survey, 180 completed the survey in 2003. The respondent pool was comprised of victims of identity theft.

Number of Prosecutions

Though there are not national survey statistics about medical identity theft prosecutions, the California Attorney General's Office, the New York Attorney General's Office, and the Pennsylvania Attorney General's office have prosecuted large cases of medical identity theft, where there was a clear intersection between health care fraud and identity theft. As a trend indicator, these prosecutions indicate at the very least the presence of a trend, if not an uptick. In California and New York, the cases involved large, complex, organized schemes involving the theft of many identities.

Conclusions regarding the medical identity theft indicators

It is not possible to draw clear, sharp conclusions from this body of statistics. However, these statistics are useful and suggest a few broad conclusions.

- Medical identity theft has been repeatedly documented as a facet of identity theft crimes.
- Medical identity theft appears to be increasing, based on the numbers available.
- Data from hotlines and census-style identity theft surveys with questions about medical use of data point with some consistency toward a number in the approximate area of 1.5 to 2 percent for rate of medically-related identity theft in comparison with other forms.
- Medical identity theft, as articulated by the numbers available, translates in number of victims in 2003 to a range of a minimum of about 3,500 victims to up to a theoretical maximum of almost 3.25 million victims. However, our best estimate is that there could be as many as a quarter to a half million people who have been victims of this crime. [36]

[35] The ITRC 2003 and 2004 surveys are available at <http://www.idtheftcenter.org/idaftermath.pdf> and < http://www.idtheftcenter.org/aftermath2004.pdf> respectively.

[36] Statistics are from the FTC Identity Theft Clearinghouse data, taken from the FTC Consumer Sentinel database. The bottom range of this figure represents 1.8 percent of 214, 905 victims, which is the percent of victims that said they experienced medical identity theft in 2003. The larger figure of "approximately

This estimate is highly uncertain because of the lack of comprehensive or firm data. Hopefully, in several years this measurement will be more precisely narrowed by additional studies on medical identity theft.

Background: General Statistics on Identity Theft

Though it is not yet a mature body of research, identity theft has begun to acquire the beginnings of some statistical information regarding its scope, mechanics, and incidence.

An early study of identity theft in 2000 by the Privacy Rights Clearinghouse and CALPIRG contained several key recommendations which later became law, for example, the report recommended that consumers have the right to one free credit report each year.[37]

Three studies, the 2003 FTC Identity Theft Survey, the BBB/Javelin Survey, and the Department of Justice survey released in 2006 are broad national studies that deserve some discussion. The FTC survey and the BBB/Javelin survey have used nearly identical survey instruments, which has provided the beginnings of a longitudinal data set on identity theft. For example:

- **2005**: The Better Business Bureau/ Javelin survey found that in the number of US adult victims of identity fraud was 8.9 million in 2005.[38]
- **2004**: The Better Business Bureau/ Javelin survey found that in 2004, 9.3 million Americans were victims of identity theft. [39]
- **2003**: the FTC Identity Theft Survey found that about 10.1 million people were victims of identity theft. [40]

The Department of Justice identity theft survey, released in April 2006, found that an estimated 3.6 million households (approximately 3 percent of all households in the nation) had learned they were the victim of at least one type of identity theft during a six-

---

3.25 million" is taken directly from the FTC 2003 Identity Theft Survey. The number represents the entire category of "New Accounts & Other Frauds' ID Theft" which includes use of identity information for medical purposes. See pages 4, 13, and Table 1. 2003 FTC Identity Theft Survey Report, September, 2003, Federal Trade Commission.

[37] Study available at < http://www.pirg.org/alerts/route.asp?id2=3683>.

[38] < http://www.javelinstrategy.com/research?cat=2>. See also <http://www.bbb.org/alerts/article.asp?ID=565> and <http://www.bbbonline.org/idtheft/safetyQuiz.asp>.

[39] < http://www.javelinstrategy.com>.

[40] Federal Trade Commission, Identity Theft Survey Report (Sept. 2003). <http://www.consumer.gov/idtheft/pdf/synovatereport.pdf>.

month period in 2004. [41] The survey instrument for this study differed from the Javelin and FTC studies.

In the future, survey instruments, particularly large ones, need to differentiate medical identity theft as a separate issue from uses of insurance information, and the survey instruments need to differentiate harms resulting from medical identity theft as separate from financial harms.[42]

Background: General Statistics on Health Care Fraud

Health care fraud encompasses many types of fraud and abuses, including but not limited to medical identity theft. It is unknown what percentage medical identity theft comprises of the fraud statistics, and it is not possible at this time to estimate that number to any degree of accuracy. This is a frustrating problem that is not new just to the understanding of medical identity theft. In 2000, Penny Thompson, the Program Integrity Director for the Health Care Financing Administration, testified about the problems of measuring fraud in Medicare and Medicaid programs. She noted:

> "Certain kinds of fraud--such as falsification of medical records--probably would not be detected through current methodology. And other kinds of fraud---on cost reports, for example--are not detectable in a claims-based sampling environment. … Fraud measurement is, in fact, uncharted territory. Our progress in pioneering payment accuracy projects might not even be directly relevant to helping us navigate this new territory. Some experts suggest that a statistically valid estimate of fraud might not be possible at all, given the covert nature and level of evidence necessary to meet the legal definition of fraud. And methods to establish fraud might be considerably different than those used to detect other payment errors."[43]

Fraud measurement is a challenging measurement environment, and the statistics that exist do not attempt to differentiate medical identity theft as a subset. This report could spend considerable pages discussing statistics detailing claims error rate and money recovered from fraud, and more. But the more useful approach at this point is to gauge how large the overall problem is, and where the trend lines lie.

Health care fraud accounts for an estimated 3 to 10 percent of all health care costs, or 80

---

[41] Katrina Baum. Identity Theft, 2004. Released April 2, 2006. (NCJ-212213). <http://www.ojp.usdoj.gov/bjs/abstract/it04.htm>.

[42] The World Privacy Forum submitted comments suggesting changes to the FTC identity theft survey instrument in response to FTC's Federal Register notice of 18 November2005, 69970, Vol. 70, No. 222 requesting input. The comments may be read at < http://www.worldprivacyforum.org/pdf/wpf_ftcidsurveycmt_fs.pdf>.

[43] Federal News Service. July 12, 2000. Prepared testimony of Penny Thompson Program Integrity Director, Health Care Financing Administration. Before the House Budget Committee Task Force on Health. Medicare and Medicaid program integrity.

to 120 billion dollars of loss per year.[44] This is a number that is so large, it is difficult to comprehend. Malcolm Sparrow, a Harvard professor who has done seminal work on understanding and quantifying health care fraud, explained the scope of the fraud problem:

> "How much gets stolen? The magnitude of the problem is measured in terms of hundreds of billions of dollars each year. How many hundreds of billions of dollars? For the time being, nobody knows for sure. If we were lucky, perhaps just one hundred billion. More likely two or three. Quite possibly four, and conceivably five." [45]

Hotline Statistics

- The Office of the Inspector General of Health and Human Services TIPS line accepts calls about health care fraud and abuse. In 1998, that line received **76,000** calls. In 1999, the TIPS line received approximately **300,000** calls. [46] Private insurers also maintain fraud tips lines, which then pass those tips to their internal investigation units.

- In 2004, BlueCross/Blue Shield plans nationwide received more than **80,000** calls to their anti-fraud hot lines, which was a **15%** increase over calls from 2003.[47]

Referrals the Inspector General's Office of HHS took Some Form of Action On

Health care fraud referrals that the Inspector General's Office of HHS took action on have risen steadily. In 2001, the IG took action on **14** percent of referrals or **77** referrals. In 2005, it took action on **30** percent of referrals, or **165** referrals. The total number of referrals the HHS Inspector General's Office has taken action on is **550**. Of these referrals, 22.9 percent were dismissed for lack of evidence of criminal intent, 17.5 percent received a Plea (District court), and 2.4 percent went to a jury trial (District court).[48]

---

[44] Government Accountability Office, May 7, 1992. T-HRD-92-29. Health Insurance: Vulnerable Payers Lose Billions to Fraud and Abuse. Statement of Janet L. Shikles, Director, Health Financing and Policy Issues, Human Resources Division. "Though no one knows for sure, health industry officials estimate that fraud and abuse contribute to some 10 percent of U.S. health care's current $700-plus billion in costs," p. 2.

[45] Malcolm K. Sparrow, License to Steal: How Fraud Bleeds America's Health Care System, at Preface (Westview Press, 2000).

[46] The Department of Health and Human Services And The Department of Justice, Health Care Fraud and Abuse Control Program.Annual Report For FY 1999. See "Beneficiary Outreach" section.

[47] "Fighting On New Fronts."October 1 2005, Best's Review.

[48] Statistics obtained by Transactional Records Access Clearinghouse using FOIA. Statistical reports were generated by TRAC for the World Privacy Forum. TRAC is a data gathering, data research and data distribution organization associated with Syracuse University.< http://trac.syr.edu/>.

Health care fraud prosecutions follow an arc that peaks in the year 2000 then drops. In 1991, 147 health care fraud prosecutions were filed by all Federal agencies, resulting in 26 convictions. Filings steadily rose and reached a peak during 2000 with 705 prosecutions filed and 471 convictions, and have broadly declined since. In 2005, 605 prosecutions were filed resulting in 516 convictions.[49]

In 2000, the median prison term for health care fraud was 5 months. In 2005, the median prison term for health care fraud was 0 months.[50]

As cited in Best's Review, BlueCross/BlueShield referred 663 fraud cases to law enforcement authorities in 2004, and 189 warrants and indictments were issued.[51]

The Human Cost of Medical Identity Theft

The evidence of harm to real people from medical identity theft is unambiguous. Victims may find themselves in situations where they suffer financial losses, are billed for services that do not actually belong to them, and more. Consider these recent cases from the FTC Consumer Sentinel Hotline dating from 2006:

- "On March 20, 2006, someone used my Social Security Number at the Primary Diagnostic Clinic at Duke University to obtain medical services and I was billed for these services. The individual did not show proof of insurance or any type of ID. I have never been a patient at any Duke facility so the bill was quite a surprise."[52]

- Another individual stated that someone "keeps putting in a change of address for him but he is not doing it." This consumer also received two medical bills for a regional medical center on his credit report that were not his.[53]

- An Indio, California resident discovered that a new medical account had been opened at a hospital in the consumer's name.[54]

- One consumer describes a nightmare of identity theft red tape: "Back in 1995 my wallet was stolen at a nearby convenience store in Elsa, Texas. There were no problems at that time until I tried to do my income tax return. They put it on hold

[49] *Ibid*.
[50] *Ibid*.
[51] "Fighting On New Fronts."October 1 2005, Best's Review. See also <http://www.bcbs.com/antifraud>.
[52] World Privacy Forum FOIA to the Federal Trade Commission. FTC FOIA-2006-00601. FTC Reference No. 8079665.
[53] *Ibid,* FTC Reference No. 8079842.
[54] *Ibid*, FTC Reference No. 8078067.

because somebody was using my Social Security Number to work at another state. ...I have also been denied credit card accounts, loans, and have been charged with accounts from another state. There is one account that I have received from Sterling ER Physicians for the amount of $339 from a collection agency that is from Trenton, New Jersey. I have never left the state of Texas .... and the person who is using my Social Security Number is receiving medical treatment."[55]

- A Texas consumer discovered that someone was impersonating them to receive employment at a packing company and at a dental office.[56]

- A concerned Houston mother called on her daughter's behalf because her daughter was billed for unknown medical services with her Social Security Number. A credit card was opened in the daughter's name. The mother believed it might be the father doing the harm.[57]

- After a car burglary, a Kentucky consumer had 7 accounts opened by an imposter. The imposter received treatment at a hospital; the bills went to collections.[58]

- A consumer found his father's personal information in his own accounts, including new medical bills and new credit card bills.[59]

- One consumer who looked at her credit report found that an imposter using her information had rented an apartment and had obtained medical services at a Washington D.C. hospital, as well as a wireless account.[60]

- A Texas consumer, after receiving her credit report, found out that the suspect had used her Social Security Number at a regional medical center for $1,650 worth of medical treatment. Her Social Security Number card had been stolen.[61]

- An Arizona man discovered two bills on his credit report that were not his – but were listed in his name. He suspected his ex-wife may have been the culprit.[62]

- A Columbus resident received a bill from a health network for services that they never received. The suspect in the case was a former girlfriend.[63]

- One consumer called to state that an imposter had used her identity to obtain a

---

[55] *Ibid*, FTC Reference No. 8078114.
[56] *Ibid*, FTC Reference No. 8077739.
[57] *Ibid*, FTC Reference No. 8077815.
[58] *Ibid*, FTC Reference No. 8079385.
[59] *Ibid*, FTC Reference No. 8078141.
[60] *Ibid*, FTC Reference No.8078943.
[61] *Ibid*, FTC Reference No. 8079056.
[62] *Ibid*, FTC Reference No. 80299279.
[63] *Ibid*, FTC Reference No. 8079611.

DirecTV account and used services at a pathology lab. The medical account was turned over to collections, and debt collectors were actively trying to collect $790 from the victim.[64]

- A Connecticut consumer reporter that someone obtained medical services at Yale New Haven Hospital in their name, using their Social Security Number. The consumer's checking account was also taken over by the imposter.[65]

- A Miami consumer whose purse was stolen told the FTC that an unknown person had obtained an AT&T wireless account, a credit card, store cards, and medical care at a regional medical center in the consumer's name. Some of the accounts had gone to collection.[66]

Financial Losses

Victims of medical identity theft may suffer financial pressures and losses. Victims have to clean up not just their medical files, but also their financial files as a result.

- In the case of a Colorado victim who had his medical identity stolen by a man who received multiple surgeries in his name, two years later he is struggling to keep his cell phone bill paid. The victim did not have insurance, and has lost property and a business due to his medical identity theft.

- One victim who wrote to the FTC said that her sister who lived with her stole her identity and used it to obtain services with Tmobile, AT&T Wireless, three different hospitals, and other businesses. This victim had financial issues to clean up, and a medical record.[67]

Harm From False Entries Put in Medical Record

Perhaps the most egregious victim stories in this area come from a Boston area psychiatrist who altered his patients' records and others' records in order to make money from fraudulent billing. The psychiatrist, for non-patients, gave them diagnoses of severe depression and in some cases drug addiction and abuse, when they were not even patients. The psychiatrist billed insurance companies for these services. Court documents from the case describe the harms:

---

[64] *Ibid*, FTC Reference No. 8079613.
[65] *Ibid*, FTC Reference No. 8079713.
[66] *Ibid*, FTC Reference No. 8079862.
[67] *Ibid*, FTC Reference No. 8079524.

> "There is no reason to believe that this misinformation will not lead to misfortune for those whose names Skodnek used in fabricating the sessions. This is an information age. While nominally confidential, these records are vulnerable to disclosure to any number of sources. Whether it should or not, the misinformation will almost certainly have an impact on patients' lives. It may determine whether an individual will be given a health insurance policy; it may decide whether he or she will receive government clearance; it may affect a whole host of other situations. ... Dr. Skodnek's abuse of trust -- and its unquestionable impact on his patients' lives and the lives of their family members -- are very, very troubling. And, what is unusual about this fraud scheme is not that Dr. Skodnek "puffed" the time he spent but went much, much further. He created a paper trail for these patients out of whole cloth, inventing histories of mental health treatment with which those individuals must now contend."[68]

This case is the best-documented case of this kind of harm. However, many victims of medical identity theft may have similar issues, they just haven't learned about them yet.

Denial of Insurance, Insurance Caps Reached

Victims of medical identity theft can be denied insurance due to imposter activity. In the Boston psychiatrist case, the doctor used up each family member's insurance one after the other until the benefits were "capped."

Loss of Reputation:

When a medical file has been altered by a suspect, it becomes an albatross around the victim's neck. A judge in the case of the Boston psychiatrist wrote:

> "The evidence suggests that once the claims were entered they cannot be deleted from the system. The most that can be done is to enter a notation in the computer records to reflect that a particular claim was false. In order to accomplish this, each member is obliged to write to Blue Cross/Blue Shield disputing the individual records. Moreover, even where a notation is entered to show that the billing record was false, the insurance carrier cannot declare--and the notation will thus not reflect --whether Skodnek's statements about diagnosis, medications prescribed and/or psychiatric symptoms of the patient were false."[69]

This is true. After falsified information is entered into a patient file, that information is in that file typically for good. Most health care providers, upon learning of a mistake in the file will correct the file. But not all will.

---

[68] United States v. Skodnek, 933 F. Supp. 1108,; 1996 U.S. Dist. LEXIS 9788 (D. D. Mass. 1996).
[69] *Ibid*.

Physician Loss of Reputation: Theft of Physicians' Identities

Physicians may experience theft of their professional identity in association with either the commission of medical identity theft, or for other health care fraud purposes. This is an area that will need to be watched carefully for any increases. It is unknown what kind of professional education is available to physicians about this issue. This report does not consider the specific challenges physicians encounter in this situation.

- A Tennessee doctor's professional identity was stolen, in that his Medicare provider number was obtained by a couple who then billed false claims in his name. The doctor's provider number and name were used without the knowledge of the doctor to obtain more than $1,000,000 in payments from Cigna Medicare.[70]

- Nurses, too may have their professional identities misused. In 2005, New York Attorney General Eliot Spitzer brought a case against a woman who had impersonated a nurse for 2 years. This case, however, was not related to a broader health care fraud case.[71]

Loss of Medical Record Privacy: Subpoenas

If an individual is a victim of medical identity theft and his or her records have been altered by a physician or another individuals, those records that have been altered may be subpoenaed for a criminal or civil case against that individual. The records can be sealed by the court, but the medical history still gets floated to more parties than a trusted health care provider.

Loss of Time

The FTC 2003 survey found that identity theft victims spent an average of 30 hours cleaning up and recovering from the misuse of their identifying information. It is unknown how many hours it will take for medical identity theft victims to clean up after the crime, but evidence suggests that it may take more time because of the difficulty in amending medical records and the time it takes to follow up with insurance companies.

How People Have Discovered They are Victims of Medical Identity Theft

[70] "Individual arrested for criminal charges with health care fraud." Federal Bureau of Investigation, Knoxville Division, press release, May 15, 2003. < http://knoxville.fbi.gov/pressrel/2003/kx051403.htm >.
[71] "Nurse imposter arrested, faces identity theft charge."Office of New York State Attorney General Eliot Spitzer, press release, August 31, 2005. < http://www.oag.state.ny.us/press/2005/aug/aug31c_05.html >.

Medical identity theft is a crime that hides itself well. It is a form of health care fraud, which, like other kinds of white-collar fraud, is not a self-revealing crime.[72] There is no way today to quantify or even guess at the percentage of victims who actually discover that their medical identities have been used fraudulently.

Statistics from the FTC address one aspect of this issue. The 2003 FTC Identity Theft Survey found that 52 percent of victims of financial identity theft discovered the misuse of their personal information "by monitoring the activity in their accounts." This included examining monthly statements from banks and credit card issuers. The World Privacy Forum did find instances of medical identity theft victims who had "crossover impact" from perpetrators who also opened credit cards in their name, or who ran up large hospital bills that went to collections. These victims may see unusual bank or credit card activity.

But the kinds of fraudulent activity that prosecutions have documented suggest that many victims of medical identity theft will not have any unusual bank or credit card activity to alert them of the problem. As a result, victims of this crime should realistically not depend only on traditional "red flags" to alert them to trouble.

Based on cases the World Privacy Forum has studied, following are the primary ways victims have discovered medical identity theft.

Collection Notices

There is a pattern in medical identity theft crimes where perpetrators change the billing address and the phone numbers on the medical charts of victims. This is particularly true when a sophisticated ring has taken over a clinic or has stolen the identity of a doctor. [73] This creates a layer of insulation for the criminals because bill collectors usually can't find the victims to alert them to a problem. But some of the "mom and pop" or "one-off" medical identity thieves can be sloppy, and this has led to some victims getting collection notices. This is what happened to a Birmingham, Alabama man. [74]

- An acquaintance of the Birmingham victim stole his expired temporary drivers' license and used it to receive emergency medical treatment in his name at several hospitals. Months later, the victim received a letter from an attorney demanding payment for an anesthesia group. The victim in this case was able to clear his name because an investigative reporter from a TV station helped him break through hospital red tape. The hospital was apparently reluctant to release the

[72] See discussion of this point in Malcolm K. Sparrow, License to Steal: How Fraud Bleeds America's Health Care System at 120 (Westview Press, 2000).
[73] Author interviews with the FBI and Department of Justice. Also see Sparrow pages 132, 133. Also see public records on cases discussed in this report. For example, See Littleton Police Department Inclusive Case Report from January 17, 2006 re: Criminal Impersonation of Joe Ryan.
[74] Medical Identity Theft: What's the Deal? NBC13.com, March 21, 2003. <http://www.nbc13.com/news/2057120/detail.html>.

medical file to the victim. But the reporter was able to convince the hospital to compare a medical x-ray of the perpetrator's and the victim's right hand – which were markedly different, and thus cleared the victim's name. The victim said his imposter's activities added up to more than $10,000 in medical bills.

- In the Ryan case in Colorado, the victim received multiple collection notices from a hospital for $44,000 worth of services he had not received. On top of that, collection notices appeared on his credit report and created a subsequent drop in his credit score. [75] In Ryan's case, he did not have insurance, so no insurance information was stolen. Even at that, Ryan's financial life has been severely impacted by the medical identity theft. In researchers' most recent discussion with Mr. Ryan, he has noted that his medical identity theft will likely cause him to lose everything "but his dog."[76]

Credit Report

Consumers whose medical bills go to collections and whose identity information is used to open multiple accounts will see that activity on credit reports. Based on consumer complaints made to the FTC regarding medical identity theft, many of those victims were alerted after seeing a credit report.

However, it should be kept in mind that there are likely many more victims who simply did not find out they were victims because the criminals did not open other accounts beyond the medical accounts.

Receipt of Someone Else's Bills

In 2005, a Lufkin, Texas medical identity theft victim received someone else's medical bills. The bills came to the victim after the perpetrator used the Texas man's identity to get medical treatment. The victim received the bills after the fact and filed a police report.[77]

One woman who complained to the FTC stated that she received a bill for her son for medical lab fees at a hospital when her son had never been to that hospital.

These incidents illustrate why its a good idea for consumers to review all bills and notices they receive concerning medical services. If there is a less sophisticated criminal, bills can tip victims off. But this is not something victims can rely on, however. Medical identity theft can be a sophisticated crime with professional operators that typically change billing addresses so this sort of thing doesn't happen. Because of the high level of

[75] See Littleton Police Department, Inclusive Case Report,Criminal Impersonation of Joe Ryan, pages 5, 6, and 11 (Jan. 17, 2006).
[76] Interview with Joe Ryan, April 2006.
[77] 5. The Lufkin Daily News, 15 July 2005, Police Report.

the criminal operators, it is more likely that victims will not know that their identities are being used.

Notification by Law Enforcement or an Insurance Company

When a fraud case comes to light, victims associated with those cases may be contacted by an insurance fraud investigator for a private insurance company, or by a member of law enforcement. In one situation like this, parents of teenagers were informed that their childrens' psychiatrist had altered their childrens' medical files to include diagnoses of "suicidal ideation" and other serious psychological illnesses that the children did not have.

Notification by a Health Care Provider

It is unusual for victims to be notified of medical identity theft by a health care provider, such as a doctor or a hospital. There have been a few reported cases, though. For example, a hospital near Albuquerque, New Mexico treated a woman for a toothache and prescribed her Oxycodone. When hospital staff called the patient to check on her condition, they discovered that the patient had impersonated her sister, and the sister's identity information had been used multiple times to obtain medical services and prescription drugs.[78]

Medical Problem at an Emergency Room

The worst-case scenario is that a victim does not learn about medical identity theft, or only learns about it during the course of a medical emergency when obvious medical discrepancies that have been introduced into the medical file by the criminal are discovered.

False entries made to the medical file is common in medical identity theft,[79] what may be less common is for victims to find out about the changes.

- In a document sent to the FTC, a Florida woman stated that she went to receive medical treatment, and said she discovered that someone impersonating her had caused false entries to be placed in her medical file. The victim was able to catch errors relating to blood type in time. [80]

---

[78] Rozanna M. Martinez ,"Ex-Deputy Is Indicted On Charges of Fraud.", 5 April 2006, Albuquerque Journal.
[79] See Jason Kandel, "Medi-Cal Fraud Flourishing on Black Market," 7 August 2005, Los Angeles Daily News.
[80] Comment of L.Weaver in Federal Trade Commission, Identity Theft Victim Assistance Workshop,(Aug. 18, 2000), <http://www.ftc.gov/bcp/workshops/idtheft/comments/weaverlind.htm>

Notification of Data Breach by a Medical Provider

Medical data breaches are serious business, because there is a long and well-substantiated history of criminals using lists of patient names in medical identity theft operations.[81] Criminals who have broken into hospital computers and have stolen patient identities for the purpose of medical identity theft may leave no other trail for victims other than a database breach notification by the breached organization.

One Jacksonville Florida consumer who complained in April 2006 to the Federal Trade Commission said that she had received a breach notification from a financial company. Later, a suspect used her name, date of birth, and Social Security Number at a dental office and charged $4,050 worth of services. The suspect also used the consumer's Social Security Number for $950 of other medical services.[82]

Medical files belonging to Oregon and Washington patients were stolen in a health system database breach in December of 2005. A Beaverton resident was quoted in The Oregonian describing a strange experience: after the breach, he received an alert from his identity theft watch service to tell him that someone was trying to reassign his phone number.[83] Changing and reassigning victim's phone numbers is a trick medical identity thieves have used to keep their victims in the dark about the crime.

This man probably did not know about how organized medical identity theft rings operate; in his case, he was fortunate to receive notification. A post-breach check of victims' credit reports will usually not reveal medical identity theft, particularly if the perpetrator is a professional, as is typical with medical identity theft. Only a proactive check of insurance claims with all relevant insurers will provide the necessary clues to victims.

Denial of Insurance Coverage, Notification that Benefits have Run Out, or "lifetime cap" Has Been Reached

Another way victims have discovered medical identity theft is when they apply for medical and/or life insurance and are denied due to diseases reflected by their altered medical charts. In other cases, victims are notified that coverage for legitimate hospital stays are being denied because their benefits have been depleted, or that their lifetime cap has been reached. Sometimes, entire families can be victimized due to "looping." Looping is a when a medical identity thief victimizes all insured members of the family one after the other, whether the victims are patients or not. After one victim's benefits run out, the thief turns to the next member of the family until those benefits run out, and so on. [84]

---

[81] Interviews with Department of Justice by author.
[82] World Privacy Forum FOIA to the Federal Trade Commission. FTC FOIA-2006-00601.
[83] Joe Rojas-Burke, "Providence critics push for safer records," January 27, 2006. The Oregonian,
[84] See, e.g.,United States. v. Skodnek. 933 F. Supp. 1108, 1996 U.S. Dist. LEXIS 9788. (D. Mass. 1996.).

Review of Explanation of Medical Benefits Notices

Some victims discovered medical identity theft when they found mistakes on their explanations of benefits notices. Medicare, Medicaid, and private insurers send these notices. In medical identity theft, the recipients' addresses may be changed, but when this is not the case, the explanation of benefits notices can be helpful detection tools.

In California, a mother checked her mentally ill son's explanation of benefits to find that Medicare had been billed for more than 70 respiratory treatments, even though her son did not have a respiratory condition. Medicare sent the son notices stating those benefits were paid, which was how this particular case came to light. The doctor in this case, which included other victims, fraudulently billed more than $7.6 million and was convicted of federal charges in 2005. [85]

Some Dynamics of Medical Identity Theft

Falsification of Medical Charts is a Root Issue

The intentional submission of false claims is the core of health care fraud, and the intentional misuse of personally identifying information is the core of identity theft. Medical identity takes elements from both crimes: medical identity theft is the intentional misuse of personally identifying information to receive medical goods or services, and it usually involves the creation of false medical records, or false entries into existing medical records.

That this happens frequently is well-known among those working in the trenches of insurance fraud. Insurance fraud investigators know that identity theft frequently leads to fraudulent insurance claims. In one case, for example, a person's insurance card was stolen and used to obtain nearly $50,000 worth of medical care.[86] The World Privacy Forum's interviews with investigators from multiple jurisdictions and agencies found that the concerns about identity theft and insurance fraud are widespread.

The prosecutor's observations were echoed by the interviews the World Privacy Forum conducted with investigators from multiple jurisdictions and agencies.

Abundant evidence exists that the creation of false records can have profound impact

---

[85] See U.S. Department of Justice "Doctor and Biller Convicted in Multi-Million Dollar Medicare and Medi-Call Billing Scam," Press Release, December 23, 2005. < http://www.usdoj.gov/usao/cac/pr2005/176.html >.

[86] US Fed News. September 15, 2005. "Office of insurance fraud prosecutor charges Newark woman with using stolen identity to commit insurance fraud." Dateline: Trenton, N.J.

which ranges from bad to potentially life-threatening. It is not unusual to find that victims' medical records have been changed to match the diseases and bodies of the perpetrator of the crime when the thief seeks medical treatment. One victim of medical identity theft, for example, showed up for medical treatment to find that her blood type had been altered in her medical files. [87]

Because medical identity theft is a crime that operates in a digital environment, hundreds or even thousands of medical records at a time may be electronically altered to support fake medical billings in get-rich-quick-schemes. Depending on the scheme, the records can be changed in damaging ways. In California, unscrupulous medical providers were caught buying Medi-Cal and Medicare patient identity numbers. The thieves were using the patient's identities to get reimbursed for millions of dollars in tests and other services that were never provided. The California Medi-Cal identity theft scam specifically involved bad actors using stolen patient information purchased for as little as $100. During interrogations, investigators learned that workers in medical records offices and billing departments had copied the information for cash. Investigators said searches had turned up medical charts in the process of being altered, with some that had been postdated or written up in a way that made no sense. [88]

No matter why or how it happens, when victims' medical files are altered, it can have negative impacts on their lives. Victims may not be able to get health or life insurance due to diseases they never had that were recorded fraudulently in their medical files. They may receive improper treatment at a hospital emergency room or other health provider that is life-threatening due to misinformation in the medical file.

Who Commits Medical Identity Theft?

Identity theft can be committed by individuals, doctors, nurses, lab technicians, organized crime rings, and more. This report does not primarily focus on the mechanics of how the crime occurred. However, it is important to note that medical identity theft is an "insider" crime more often than not, and frequently involves health professionals at some level. One Medicaire/Medicaid fraud investigator interviewed for this report went so far as to say that the crimes she saw always had a component of a medical professional being involved. Sometimes, even the doctors are victims of identity theft; one of the mechanisms of medical identity theft in organized crime is to use a legitimate and innocent doctors' identity to steal patient identities.

---

[87] Federal Trade Commission, <http://www.ftc.gov/bcp/workshops/idtheft/comments/weaverlind.htm>. August 18, 2000.

[88] See Jason Kandel, "Medi-Cal Fraud Flourishing on Black Market," 7 August 2005, Los Angeles Daily News.

Organized Crime

Organized, complex schemes have been discovered in California, Florida, and New York. In the hands of organized crime, false claims are spread out across multiple patients, and the claim amounts are small. Malcolm Sparrow describes this process in his book, License to Steal:

> "Most large fraud schemes are deliberately constructed around larger numbers of smaller claims (to avoid arousing suspicion.)"[89]

Organized patterns of this crime tend to involve what is called "*clinic takeover*." This is where a group purchases a small clinic, operates the scam out it for a few months to a year, then shuts the operation down and disappears. The clinic may or may not be staffed with real doctors. Clinic takeover is particularly insidious because patients get taken into a slick scam and may have no idea that there was every a problem. Victims of clinic takeovers may in some cases be visiting clinics where each person they see there is involved in some way with the crime.[90]

Solo Identity Thieves

Lone identity thieves do commit medical identity theft. So far, the pattern appears to be that of a seasoned criminal committing the crime. Occasionally, an individual with no criminal background but who is desperate for health insurance will commit this crime. This occurred at the University of Connecticut. In that case, a man with AIDs used his cousin's health insurance information to receive approximately $76,000 worth of treatment.[91]

The more experienced the criminal, the more likely they are to have acquired a fake driver's license. This was the situation in a case in 2000 where a San Diego man used one victim's identity to commit financial identity theft and to receive medical treatment while he was impersonating the victim.[92]

---

[89] Malcolm K. Sparrow, License to Steal: How Fraud Bleeds America's Health Care System, at 51 (Westview Press, 2000)

[90] U.S. v. Dzugha, Case 5:05-cr-00589-JF (N. Cal). Indictment, pages 4 –7.

[91] Interviews with hospital staff members, also see University of Connecticut Advance, "Steps taken to stem healthcare identity theft," September 7, 2005. <http://www.advance.uconn.edu/2005/050907/05090711.htm>.

[92] "FBI announces indictment and arrest in a case of identity theft," Federal Bureau of Investigation San Diego Division press release, March 8, 2000. < http://sandiego.fbi.gov/pressrel/2000/berend.htm>.

Doctors and Other Health Care Providers

Doctors can be involved in medical identity theft schemes. This does not represent the majority of doctors, rather it represents only a small percentage of bad actors. There are numerous ways the "bad actor" doctors have been involved. Some operate alone, some "rent" their license information to scammers, and some operate as the legitimizing factor for organized "clinic takeovers."

One example of this occurred during 1995 to 1996. Six individuals who took over a clinic in Miami for a period of about a year submitted $6.5 million in claims, including claims for beneficiaries who never went to the clinic for services. The way the scheme operated was in cooperation with legitimate doctors who sold their medical licenses and provider numbers to the clinic.[93]

Relatives of beneficiaries

As in financial forms of identity theft, there are cases where siblings and extended family members have taken over the identity of an individual within the family. The University of Connecticut case is one example of this, as is the New Mexico case where a hospital near Albuquerque, New Mexico treated a woman for a toothache. When hospital staff called the patient to check on her condition, they discovered that the patient had impersonated her sister, who lived in the area. [94]

Opportunists

Individuals who work in settings where there is a lot of patient data may be tempted by the quick money medical identity theft provides. The pattern here is for people who have insider access to doctor's offices or hospitals to copy patient information and sell it, or to use that information to help provide victims for more organized medical identity theft schemes.

Medical Identity Theft is a Crime that Hides

The reason health care fraud is so difficult to track is that the crime hides itself well. Sparrow has commented on this issue:

> "With health care fraud, as with many other forms of white collar crime, what you see is not the problem. The problem, by its very nature, is largely invisible, and

[93] "Arrests made in $6.5 million Health Care Fraud Scheme," Office of the Attorney General of Florida press release, November 23, 1999.
[94] Rozanna m. Martinez, "Ex-Deputy Is Indicted On Charges of Fraud" 5 April 2006, Albuquerque Journal..

> we make a grave mistake if we inform ourselves about the problem only by paying attention to what comes to light." [95]

Financial identity theft -- such as situations where a thief takes over a victim's credit card account or uses the victim's information to create new accounts -- typically reveals itself on the victim's credit card or in the victim's credit report. Additionally, credit card companies and other financial institutions have sophisticated fraud detection systems that flag fraud attempts in real-time. Many people who use credit cards can identify a time that they received a phone call from a credit card company asking about "unusual activity" on their cards. As a result of these and other tools, quite often, victims of financial identity theft may discover the crime if they are paying enough attention. Currently, there are a number of mechanisms such as free credit report checks that help victims do just that.

Recourse and Recovery Issues for Victims

Victims of medical identity theft may need help with recovery in the area of correcting medical files and insurance records. They may also need help in the area of correcting financial information. In the area of financial recovery, multiple excellent resources exist for consumers. But in the area of medical and insurance information correction and recovery, victims will not find nearly the same resources or availability of recourse.

Financial Recovery Tools are Available for Victims

Multiple high-quality resources and pathways of recourse exist for victims of financial forms of identity theft. The Federal Trade Commission has dedicates resources to this area, and offers clear, effective tips for consumers. For example, the FTC maintains a consumer identity theft information page[96] < http://www.consumer.gov/idtheft/> which contains a four-step plan for recourse. Consumers have a statutory right to receive one free credit report from each of the three main credit reporting bureaus once per year.

Victims of medical identity theft may also experience in addition to the medical identity theft the full range of financial identity theft. In these cases, medical identity theft victims can use the available tools for financial identity theft victims and at the very least work to achieve recovery in that area.

---

[95] Malcolm K. Sparrow, License to Steal: How Fraud Bleeds America's Health Care System, at 51 (Westview Press, 2000)

[96] <http://www.consumer.gov/idtheft>

Correcting and Recovering from the Medical and Insurance Aspects of Medical Identity Theft is Difficult

The high-quality tips and resources and the rights afforded to victims of financial forms of identity theft do not extend to the medical and insurance aspects of identity theft crimes. Victims of medical identity theft may generally experience multiple difficulties in attempting to recover.

The primary challenges include:

- Lack of enforceable rights to correct medical records in all instances.
- Lack of a government agency dedicated to help victims of medical identity theft.
- Lack of enforceable rights to delete misinformation from medical records.
- Lack of ability in most cases to find all instances of medical records.
- Lack of information resources about the unique needs of medical identity theft victims.
- Lack of a government agency dedicated to help victims of medical identity theft.

Why Can't Victims Correct Their Medical Records?

The federal health privacy rule issued under the authority of the Health Insurance Portability and Accountability Act (HIPAA) gives an individual (e.g., a patient or an insured individual) the right to seek amendment of their medical records. However, that right has some significant limitations. The right to ask for an amendment does not apply to medical information that was not created by the provider or insurer currently maintaining or using the information.[97]

This means that any medical information sent by one provider or insurer to another provider or insurer does not have to be corrected by the recipient of the information, even though that recipient is using the information to make decisions about the record subject. HIPAA does not prevent an entity covered by the law from considering a request for amendment of a records provided by a third party, but an individual cannot even use the limited force of HIPAA to compel consideration of a request for amendment.

In medical identity theft, victims can get trapped in a maze of blame-shifting and

[97] 45 C.F.R. §164.526(a)(2)(i). Some state laws may allow a right of amendment that does not include the HIPAA exclusion for third party records.

circularity. If a doctor or hospital submitted an incorrect record, the insurance companies have no requirement to correct those medical files. The doctor in some cases may correct the file, but that does not ensure that all copies of the file (for example at labs) get corrected. And in cases where doctors have committed the identity theft or were part of the theft, it is nearly an impossibility to get the records corrected after the fact.

In short, anyone who is a victim of this crime may have an extremely challenging time trying to get medical files corrected, even if there are life-threatening changes on those files. The shift from paper files to electronic files has exacerbated this problem: victims of this crime may never be able to find each and every copy of their medical file, much less get it corrected. This can be especially problematic if the file was primarily an electronic file with no paper backup and did not have adequate audit and security controls. Hospitals or other providers may refuse to show the victim the medical file that was fraudulently created by the thief, even if the file has the victim's name on it.

In some reported cases, an individual may not be able to see the record in the first place. Hospitals or other providers have in some cases refused to show the victim the medical file that was fraudulently created by the thief, even if the file has the victim's name on it. [98] The HIPAA right of access may help, but if a patient argues that the information cannot be about himself, a hospital may be unwilling to disclose the records. A patient could be stuck in a Catch-22, where the patient cannot see the record in their file because the patient claims not to be the subject of the information.

The reason for the HIPAA limitation on amendment of information provided by a third party originated with legitimate a concern that the holder of information may not have the knowledge to make a decision about the correctness of the information. However, the HIPAA limitation provides no recognition of the problem faced by medical identity theft victims.

To illustrate the sweep of the HIPAA amendment limitation, consider how the same policy would work for financial identity theft. The Fair Credit Reporting Act as amended grants access and correction rights to subjects of credit reports held by credit bureaus ("consumer reporting agencies"). All of the information found in a typical credit report comes from third parties and does not originate with the credit bureau. Thus, if the HIPAA amendment limitation applies to credit reports, a financial identity theft victim would have no ability to change a credit report. Instead, however, the FCRA imposes on the credit bureau has to conduct a reasonable reinvestigation to determine if the disputed information is inaccurate.[99] The FCRA establishes a procedure that defines the role of the credit bureau (and of a furnisher of information[100] to a credit bureau) that seeks to find a reasonable balance among all of the interests involved. HIPAA essentially washes

[98] The World Privacy Forum is aware of two instances where this has occurred. See Littleton Police Department Inclusive Case Report, March 25, 2004 (Case 2004001789) and "Medical identity theft:What's the Deal?" March 21, 2003. NBC13, Birmingham, Alabama.
<http://www.nbc13.com/nbc13investigators/2057120/detail.html>.
[99] 15 U.S.C. § 1681i(a)(1)(A).
[100] 15 U.S.C. § 1681s-2.

its hand of the problem with an overly broad exemption.

In an October 2005 press release HHS Secretary Mike Leavitt said:

> "Given what we recently experienced with Hurricanes Katrina and Rita, the need for portable patient information that can follow the patient has never been more important." [101]

From a perspective of a system with zero fraud and zero medical identity theft, this would make sense. But given the realities of these crimes, this "all records in any city" perspective means that medical errors introduced by criminals and unable to be corrected by victims will be endlessly perpetuated. Further, it is possible that a network will contain information for which no identifiable organization has responsibility to consider amendments. Everyone with access to the network may claim that someone else is responsible in order to avoid the expense and complication of handling amendments.

Medical Identity Theft and HIPAA

The HIPAA legislation and privacy rule were written at a time when medical identity theft was not foremost on the minds of policymakers. While health care fraud as a general issue was definitely on lawmakers minds (as is evidenced by the specific anti-fraud provisions in HIPAA), medical identity theft and its specific consequences were not.

One provision in HIPAA, which is called the *Accounting of Disclosures*,[102] could possibly be helpful for some victims of medical identity theft in some circumstances, but it too has exceptions that limit its utility.

HIPAA and Accounting for Disclosures

The HIPAA privacy rule requires covered entities – such as a health care provider -- to maintain an accounting for disclosures. An accounting contains a history of disclosures that have been made by the covered entity. The accounting is useful because it allows a covered entity to send amendments to any person who previously received information determined to be incorrect. In addition, the HIPAA accounting requirement allows a patient to ask any covered entity to provide a copy of the accounting.

While this provision might be of particular use to the victim of medical identity theft, the exceptions to the requirement render it almost useless. A covered entity is not required to maintain any accounting of disclosures for disclosures for treatment, payment, or health

---

[101] "HHS Awards Contracts to Advance Nationwide Interoperable Health Information Technology - Strategic Partnerships with Public-Private Groups Will Spur Health IT Efforts." 6 October 2005. U.S. Health & Human Services Documents. <http://www.hhs.gov/news/press/2005pres/20051006a.html>.
[102] 45 C.F.R. § 164.528

care operations.[103] This restriction may make it impossible for a patient to track the flow of medical information to and from sources that may perpetrators of identity theft.

The rule (45 C.F.R. § 164.528) has attracted plenty of criticism from covered entities that it is too costly or too difficult to implement. It its 2006 State of HIPAA Compliance Survey, the American Health Information Management Association wrote the following:

> "As in previous years, the accounting for disclosures requirement is reported to be a difficult one and is most often mentioned as needing modification. AHIMA and other groups have sought a recommendation for such an amendment from the National Committee on Vital and Health Statistics and the Office for Civil Rights, but at this time no amendment is expected in the near future." [104]

In response to complaints about the accounting requirement, the Office of Civil Rights has publicly but unofficially stated that it is considering eliminating the accounting requirement altogether or changing it. [105] Eliminating the accounting requirement would be counterproductive, and would serve to ensure that consumers never found out where their health records have gone.

It is readily apparent that health care record keeping will be increasingly automated and networked in the future.[106] This prospect, especially the increased networking, means that the risks of improper access to and disclosure of records will increase in the future.[107] This report has abundantly discussed the consequences of improper access to patient medical information. The U.S. government and its agencies such as HHS must find a way to control improper uses and disclosures. A thorough accounting of disclosures is one way to accomplish that goal.

HHS officials have touted the benefits of digitized environments. One benefit of a digitized medical health care environment is that maintaining accounting is a relatively simple task provided that the capability for accounting is built into the system at the beginning and not added on later. Indeed, many automated health record systems installed today already include a capability for accounting for all uses and disclosures and

---

[103] 45 C.F.R.§164.528(a)(1)(i).
[104] 2006 State of HIPAA Compliance, p. 14. Available from < http://www.ahima.org/index.asp>.
[105] For example, at the September 2005 HIT/HIPAA summit in Washington DC, a representative from the Office of Civil Rights made such a statement in a panel discussion on the topic.
[106] A national campaign toward modernizing, digitizing and automating health care records is currently underway, as are plans for the creation of a national networked architecture to manage those records (the NHIN.) See, for example, Executive Order 13335, "Incentives for the Use of Health Information Technology and Establishing the Position of the National Health Information Technology Coordinator" (Washington, D.C.: Apr. 27, 2004). Also see the Office of the National Coordinator for Health Information Technology (ONC) <http://www.hhs.gov/healthit/`>.
[107] For a more detailed discussion of these issues, see the World Privacy Forum testimony on Electronic Health Records (EHRs) and the National Health Information Network before the Privacy and Confidentiality subcommittee of the NCVHS. See in particular the discussion of medical identity theft and the security issues related to the NHIN.
<http://www.worldprivacyforum.org/testimony/NCVHStestimony_092005.html>.

not just those required by the HIPAA rule. [108] Health care providers should include accounting in automated systems not just because of the rule, but because it is good a record keeping policy that protects the provider as well as the patient. The federal government has operated under the Privacy Act of 1974 for many years, and no problems with accounting for health care disclosures have been reported.

A better approach would be to have a universal accounting rule covering all disclosures without any exceptions. Accounting for uses (accesses within the institution maintaining the records) would also be helpful to record subjects and to record keepers. A full, robust data accounting architecture and system should be an essential element of any National Health Information Network (NHIN). With sufficient notice, system vendors will be able to meet any accounting requirements at marginal cost.

Whether the HIPAA accounting rule was an unreasonable burden when imposed on paper or computer systems that did not already include the ability to do accounting is an open question. However, for any computerized system of health records – and certainly for any computer system established in the future and certainly for any network – accounting should be a universal requirement for all disclosures and for all internal uses as well. No exceptions to accounting should be permitted when the accounting can be accomplished automatically and inexpensively by well-designed software designed in advance to meet a requirement.

The Security Issues This Crime Raises

Medical identity theft brings forward pronounced security issues for the medical world, including issues related to data breaches, physical security issues, and other security issues.

Data Breaches and Medical Identity Theft: Data Breach Notification Needs to go to Each Individual Impacted

Given the evidence that sophisticated criminals are working in the area of medical identity theft, it is reasonable to conclude that the data breaches targeting hospital systems with rich patient and insurance data may well lead to patient information being used without patient consent or knowledge.

Individuals must be informed directly anytime their protected health information is inappropriately accessed. If individuals are not notified of a breach, then they may not

[108] Many tools have become available to facilitate HIPAA compliance, including software and enterprise systems designed specifically for the automating of accounting of disclosures. See among many examples, HIPAA Guard by Integritas < http://www.integritas.com/>, which is a paperless accounting of disclosures system, Etrack Disclosure Tracking System. < http://www.hipaarx.net/products_disclosures.htm >, Cortrak http://www.cortrak.com/, HPATS by IO Datasphere, among many others.

know that their medical files may be being altered by criminals in ways that may threaten their health, impact their insurability, or cause other harms. Because of a lack of studies in the area of medical identity theft, we do not know how many medical identity theft crimes go undetected. Data breach notification is one way to ensure that breach victims begin to monitor their insurance information closely.

Since 2005, some health care providers have given notice to consumers when there is a data breach involving sensitive or protected health information, depending on state laws.

For example, in January 2006, Providence Health System notified individuals of a data breach.[109] It is not unusual for the health care provider to follow up with a "post-breach study" of victims to determine if there has been any incidence of identity theft. Companies such as ID Analytics and others have acquired expertise in analyzing credit report activity and other indicators to make this assessment. While breach assessments have been helpful for victims of financial identity theft, the same may not necessarily hold true for victims of medical identity theft.

New Polling Methods for Post-Breach Studies are Needed

Medical identity theft may not always reveal itself like standard financial identity theft, and as a result, it has not always been identified in follow-up studies of data breaches of medical data. One of the questions that could be asked to begin to develop a more effective methodology for victims of identity theft would be to poll insurers to see if there are claims made in the victims' names. This kind of polling is expensive, because the individual victims need to be interviewed as well. Victims may be the only ones who can tell if a medical service billed to an insurer in their name was really a service that they received or sought.

The National Health Information Network and Medical Identity Theft

A number of well-intended individuals and organizations have claimed that making all health records electronic and implementing the NHIN will reduce costs, save lives, and reduce fraud. This report does not consider the cost claims of the NHIN. However, this report has considered the claims of the HHS and others that the NHIN will reduce fraud and save lives.

Here are, in brief, the scenarios that HHS officials envision due to the NHIN:

- The NHIN will save lives because medical records for everyone will be online,

[109] Joe Rojas-Burke, "Providence critics push for safer records." The Oregonian, January 27, 2006.

and will be available everywhere.

- The NHIN will save lives because there will be no more medical errors when medical records are digitized and put online.

- The NHIN will reduce fraud because it will be easier to analyze records when they are in digital form.

It would be difficult to find a person who would not desire for these statements to be true. However, due to the presence of medical identity theft and other forms of fraud from within the system, these statements cannot be and are not supported by the current facts.

The GAO, in a 48-page report published in February 2006 about the problems with information security at Health and Human Service in its existing health information systems such as Medicare (among others) wrote:

> "Information system controls are a critical consideration for any organization that depends on computerized systems and networks to carry out its mission or business. Without proper safeguards, there is risk that individuals and groups with malicious intent may intrude into inadequately protected systems and use this access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks."[110]

This statement is an excellent summary of the problem that already exists in Medicare/Medicaid, and it is a potent harbinger of what the NHIN will face.

The Lessons the NHIN Needs to Learn from the High Incidence of Fraud in Medicare / Medicaid Electronic Systems

The Office of the National Coordinator for Health Information Technology[111] commissioned a report to look at fraud in the NHIN. The report concluded that the NHIN could be used to reduce fraud.[112] One of the suggestions in the report was that data required from the NHIN for monitoring fraud and abuse must be derived from its operations and not require additional data transactions.[113] In light of all the studies of fraud in the already-digitized Medicare systems, this is an assertion that needs to be reevaluated. If this model is indeed incorporated, this recommendation may ensure that medical identity theft would not be caught by the system. This is something that has already been shown in the Medicare systems.

---

[110] Government Accountability Office, INFORMATION SECURITY: Department of Health and Human Services Needs to Fully Implement Its Program at 5 (GAO-06-267), (2006).
[111] The Office of the National Coordinator is part of the Department of Health and Human Services. See < http://www.hhs.gov/healthit/>.
[112] Nikki Swartz, "E-Records May End Fraud." 1 January 2006. Information Management Journal.
[113] *Ibid*.

Medicare/Medicaid systems are highly digitized. That is how HHS handles more than a billion health care claims each year: the majority of those claims are auto-adjudicated. A voluminous number of excellent studies have been conducted on fraud within the electronic systems of Medicare and Medicaid. At this point, prominent researchers have concluded – based upon the factual evidence – that the electronic environment has greatly contributed to the fraud problem in those programs. [114] There is no reason to think that the NHIN will not be subject to these same dynamics.

A February 2006 GAO report looked at Medicare Claims Processing Systems. These are the CMS contractor-operated group of systems that are used to process Medicare claims. These processing systems include inpatient hospital care, nursing facilities, home health care, and other health care services. The GAO investigation found significant weaknesses in information security.

> "Significant weaknesses in information security controls at HHS and at CMS in particular put at risk the confidentiality, integrity, and availability of their sensitive information and information systems. HHS has not consistently implemented effective electronic access controls designed to prevent, limit, and detect unauthorized access to sensitive financial and medical information at its operating divisions and contractor-owned facilities. Numerous electronic access control vulnerabilities related to network management, user accounts and passwords, user rights and file permissions, and auditing and monitoring of security-related events exist in its computer networks and systems. In addition, weaknesses exist in controls designed to physically secure computer resources, conduct suitable background investigations, segregate duties appropriately, and prevent unauthorized changes to application software. These weaknesses increase the risk that unauthorized individuals can gain access to HHS information systems and inadvertently or deliberately disclose, modify, or destroy the sensitive medical and financial data that the department relies on to deliver its vital services."[115]

If the HHS systems reveal systemic weaknesses such as that which the GAO discovered, then how can another system that HHS is overseeing be substantively different?

Current Audit Systems Do not Resolve The Problem

One 2002 article advocated that to combat health care fraud, that automation was the answer, and that consumers should not be allowed privacy protections that allow opting out of automated regimes. :

---

[114] The most definitive technical and operational analysis of these systems has been written by Malcolm K. Sparrow in License to Steal: How Fraud Bleeds America's Health Care System, at chapters 5-8 (Westview Press, 2000)

[115] GAO-06-267, p. 2.

> "Automation can also reduce fraud and abuse by carefully tracking providers' reimbursement claims and matching those claims with electronic treatment records. To effectuate these savings, national privacy policies should encourage consumer and provider participation in electronic filing techniques, and avoid measures that would limit potential savings (e.g., privacy protections that allow consumers to "opt out" of computerized health databases)." [116]

What the authors may not have taken into consideration is that particularly in medical identity theft, comparing a fake billing record with an equally fake electronic treatment record only proves that the slick criminals lied two times. This pattern of "lying twice" is the norm in medical identity theft, and this proposal of automated checking would do nothing to prevent or even detect medical identity theft, particularly the variety that introduced life-threatening changes to health records.

Thoughtless automation is not helpful in prevention. And automation that does not have rigorous security enhancements and audit trails can introduce new challenges into the environment.

Digital Security Issues in the NHIN and Other Highly Digitized, Virtualized Environments

The medical environment poses unique challenges for anyone attempting to provide meaningful security against crimes such as medical identity theft. In a financial environment such as a bank, the structure and idea of defense is to erect an impermeable perimeter with a membrane that only the right people (such as legitimate account holders) can get through – using such tools as two –factor authentication and so on. Auditing tools and protocols can strictly control and track insider access.

But in a medical environment, this sort of moat and castle security architecture is not realistic. The larger the medical environment, the more complex the virtualization will become. Hospitals may have multiple ports of data access and dissemination, including mobile devices such as PDAs. Some hospitals are increasingly using RFID tags to interface with wireless LANs and to create "sensor space" where blood, equipment, and sometimes even patients are tracked electronically through the hospital.[117] Etherealized patient data can be picked up not from one terminal, but from wireless entry points, RFID bracelets and anklets, PDAs, paper charts, and in some structures, remotely from laptops

---

[116] Lawrence O. Gostin, James G. Hodge, Jr , Modern Studies in Privacy Law: National health information Privacy regulations under HIPAA: Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule, 86 Minn. L. Rev. 1439 (2002).

[117] Business Wire. February 9, 2005 Wednesday 5:07 PM GMT. "University of Chicago Comer Children's Hospital Selects Mobile Aspects." Also see "System targets blood-type mix-ups," The Boston Globe, 24 February 2005. Scott Allen. Also see "Ubisense Ultrawideband Location Devices Certified by US FCC Approval Opens U.S. Market for Location Aware 'Smart Space' Platform, Ubisense one of the First Companies to Receive Certification." PR Newswire (U.S.) 06 December 2004.

in doctor's homes.[118] And finally, that patient data, if housed on a network, may be generated amongst dozens of other hospitals, crossing state lines.[119] In one NHIN scenario outlined by HHS, the patient data could be potentially remotely accessed from any hospital or provider connected to the NHIN, no matter what city the patient is in. [120]

The security issues go further and deeper, though, than just display of data. Medical information has to be moved across software and hardware, and sent off to multiple third parties such as insurers, labs, and so forth, thus infinitely making more complex the security issues. These profound security issues, which have no simple or easy or even a perfect answer, must be seriously and rigorously considered in the context of medical identity theft. To do any less is to jeopardize patient safety and health, and ultimately, the integrity of medical research based on patient data.

Physical Security Issues in a Medical Environment

One of the most challenging issues in a medical environment is to physically secure data. In a provider environment such as a hospital, where a few seconds or minutes may mean the difference between life and death for a patient, the emphasis is correctly on speed and ease of access to information. And therein lies the extraordinary challenge of securing patient data in the health care environment.

How does an organization or provider go about meeting health and safety goals while meeting security goals that also impact health and safety? These two issues are at odds, and to date there have not been mature enough solutions that fully meet both needs. In even the most rigorous, responsible environment, there will be a tension. In environments where there or a lack of attention to security issues, various types of disasters ensue.

One recent example occurred in Sacramento. There, at an HIV/AIDs clinic, a laptop containing the health information for 1,764 clients was stolen in a home burglary. The computer records include the name, age, gender, race, ZIP code and HIV status of nearly every CARES client. The files do not include addresses, Social Security numbers or driver's license numbers.A researcher had brought the computer home to do some work.[121]

Other examples include:

---

[118] See: "Company receives product leadership award for patient ID wristband." Biotech Business Week, 20 December 2004. Also see "AXCESS ActiveTag Product Tapped for Patient ID System." 17 February 2005, Wireless News.

[119] HHS Awards Contracts to Advance Nationwide Interoperable Health Information Technology - Strategic Partnerships with Public-Private Groups Will Spur Health IT Efforts. 6 October 2005, U.S. Health & Human Services Documents.

[120] "HHS Awards Contracts to Advance Nationwide Interoperable Health Information Technology - Strategic Partnerships with Public-Private Groups Will Spur Health IT Efforts." 6 October 2005, U.S. Health & Human Services Documents. See also Robin Blair, RHIO Nation, 1 February 2006, Health Management Technology.

[121] Todd Milbourn , "Stolen laptop contains files on HIV patients", 23 February 2006. The Sacramento Bee.

- A CMS Medicare contractor used a privately owned vehicle and an unlocked container to transport approximately 25,000 Medicare check payments over a 1-year period. [122]

- Four hundred forty individuals were granted unrestricted access to an entire HHS data center, including a sensitive area within the data center— although their job functions did not require them to have this level of access.[123]

Insider Aspect of Medical Identity Theft is a Fundamental Security Issues for the NHIN and other Health Care Systems

Based on the known cases of medical identity theft and health care fraud, many medical identity theft cases have an insider aspect to them. This is true in the private and in the public sector.

The GAO wrote:

> " …. it has long been recognized that the greatest harm to computing resources has been done by authorized individuals engaged in improper activities— whether intentionally or accidentally.[124]

There is a percentage of medical identity theft that occurs by siblings or by individual criminals without insider access. But the current evidence strongly indicates that people with legitimate access to computer systems and/or patient data may often be the primary culprits.[125]

In one case brought in Texas, a woman was sentenced for identity theft. She stole patient information she found while working in a medical billing department.[126] In another case, an individual who worked in an intermediate care unit at a hospital in Alexandria, Virginia was charged with used her position in the hospital to take protected patient information, photocopy, and then pass it off to an accomplice or use it for her own purposes.[127]

Of all the security issues raised by medical identity theft as a whole, other than the harm to victims and to the medical system , the insider nature of the crime is likely going to be

---

[122] Government Accountability Office, INFORMATION SECURITY: Department of Health and Human Services Needs to Fully Implement Its Program at 12 (GAO-06-267), (2006)..

[123] *Ibid*.

[124] GAO-06-267 HHS Information Security

[125] See discussion of cases in this report for examples.

[126] "Defendant sentenced in identity theft scam." U.S. Department of Justice press release, United States Attorney Northern District of Texas. August 19, 2002. < http://www.usdoj.gov/usao/txn/PressRel02/thompson_cynthia_sen_pr.html >.

[127] News Release. U.S. Department of Justice. United States Attorney Eastern District of Virginia, July 21, 2005.

the most intransigent to correct. While a bank may use internal audit trails to log and monitor insider access, in a medical environment that depends on a high amount of interaction between people, the same kinds of controls are not likely to be as effective.

What's Next? Going Forward From Here

The Necessity of a Comprehensive Risk Assessment

Risk management and anti-fraud experts have not been visibly included as stakeholders in the NHIN process. Robert Charette is the chair of the ISO/IEEE Standard on systems and software engineering risk management, and is the president of a company that specializes in enterprise risk management. As an expert who understands the risk of the proposed NHIN, he wrote a thoughtful commentary expressing his frustration with the lack of a clear, systemic planning effort or vision for finding, anticipating, and mitigating risks in electronic health care systems.

> "What disturbs me most is that I don't see any comprehensive risk management plan for this effort, nor do I see much in the way of a desire to define one. As anyone who has been involved in large-scale endeavors, managing the risks involved from a total enterprise perspective is absolutely vital to achieving success. If the NHIN is so critical to the nation, if it will radically transform health care in this country, shouldn't there be at least some systemic risk management plan with the risks defined, prioritized and where possible, mitigated?
>
> Since new systems always introduce unexpected problems, such potentially perverse consequences also need to be part of such a plan. … for example. What could happen if a large number of poorly implemented EHR systems get interconnected?" [128]

Charette is correct on this point. Going further, it is reasonable to say that there has been a lot of sales pitches for the NHIN and electronic health records, but there have not been reality checks such as those Charette is wisely bringing forward.

Legitimate Drug Trials and Medical Researchers Need to Differentiate Themselves From Fraudsters

It is likely to become increasingly difficult for the estimated 2 million patients who participate in medical research to discern what is a medical identity theft scam and what is a legitimate drug trial or medical research opportunity. An Associated Press article

[128] Robert Charette, "What Happened to Do No Harm?" 1 April 2006. CIO Magazine..

described how the recruitment of clinical test volunteers now includes glossy advertising techniques and old-fashioned in-person recruiting techniques:

> "A visit to Las Vegas with her husband to attend his funeral director convention led her to an Alzheimer's information booth. Becker, 68, of Struthers in northeast Ohio, is now among the approximately 2.3 million Americans who participate annually in medical testing. …Recruiting test volunteers isn't left to chance. There's a growing array of outreach programs, including focused advertising, glossy brochures and a renewed emphasis on basics such as a high-visibility recruiting table of the kind that caught Mrs. Becker's attention. Hospitals also look for participants among their visitors and at stores and retirement parties."[129]

Byron Hollis of the of Blue Cross /Blue Shield described in a magazine interview how "Fraudsters, posing as nurses, go door-to-door looking for seniors who need health-care. Instead they collect Medicare and Medicaid numbers and bill the government for services they never provide."[130]

Medical identity theft scams are also online. World Privacy Forum researchers located the following ad in an online Brooklyn, New York classifieds ads:

> **"Free medical exams**! Please bring with you: • NYS or Federal Picture ID and Social Security Card • 3 letters of reference with name and phone number • Original HHA/PCA Certificate (if you have one) • Proof of address (bill or lease in your name. If you do not have a bill or lease in your name you must write a letter stating who you live with, notarize the letter, and bring that persons bill or lease) • Recent Medical Examination results including PPD, Physical, Rubella and Rubeola. If you do not have a medical examination we will provide one at NO COST to you."[131]

It is possible that this ad was not for a medical identity theft scam. But the ad does have certain medical identity theft flags, including the offer of a free medical exam, and an overt request for a great deal of personally identifying information. Blue Cross /Blue Shield specifically warns its beneficiaries about these kinds of scams. The BCBS web site advises consumers to " Be cautious of free medical exams, co-payment waivers, or advertisements stating "covered by insurance."[132]

---

[129] Thomas J. Sheeran, "Volunteers sought to aid medical studies." April 7, 2006. Associated Press.
[130] Fraud Magazine, Association of Certified Fraud Examiners. March/April 2006. "Health-care fraud drains lifeblood from patients, system. Interview with Byron Hollis, Esq., CFE, AFHI, National Anti-Fraud Director of Blue Cross Blue Shield Association."
[131] Found at http://www.wynn.com/bol/classads/.
[132] <http://www.bcbs.com/antifraud/>

Further Study: Getting a Grasp of the Size, Scope, Incidence of This Problem is Crucial

Currently, sharp, clear numerators for medical identity theft do not exist. There is too much that is not known because it has not been studied. In order to develop adequate and effective prevention and detection of this crime, its incidence, prevalence, and so forth will need to be quantified.

Currently, some providers are checking a passport or drivers' license at points of entry to the healthcare system, such as at doctor's offices and hospital emergency rooms. This will catch the most desperate and least professional thieves, but it will do nothing about the fraud that occurs because a crime ring has stolen a dozen doctors' identities, hundreds of identities belonging to the doctors' patient rosters, and is systematically billing and changing medical files without ever stepping foot in the health care provider's office or seeing a single patient.

New Consumer Tips for Medical Identity Theft Victims

Based on the cases of medical identity theft that have come to light, it is possible to articulate some advice specifically tailored to victims of medical identity theft.[133] This advice includes the following recommendations:

- Closely monitor any "Explanation of Benefits" sent by an public or private health insurer. If anything appears wrong, raise questions with the insurer or the provider involved. Do not assume that things are okay just because you don't owe money.

- Once a year, pro-actively request a listing of benefits paid in your name by any health insurer that might have made payments on your behalf.

- Request annually (or more often if there is a specific cause for concern) an accounting of disclosures from health care providers and health insurers.

- Request a full copy of current medical files from each health care provider.

---

[133] Victims of medical identity theft who also experience financial consequences should see the following thorough resources for dealing with this aspect of the crime: Federal Trade Commission <http://www.ftc.gov>; Privacy Rights Clearinghouse <http://privacyrights.org>; Identity Theft Resource Center <http://www.idtheftcenter.org>.

- If a healthcare provider, for example, a hospital, refuses to release medical files that are in your name, file an appeal under HIPAA at the hospital. File a complaint with the Office of Civil Rights at the federal Department of Health and Human Services if you are not satisfied. Consider seeking assistance from state health departments, fraud investigators elected representatives, or lawyers if you believe that the denial of access may be covering medical identity theft.

- If you discover your medical or insurance records contain false information, work to amend those records. If you find information that is not about you or that bears no relationship to treatment that you did not receive, demand that the false information be removed entirely from the record.

The World Privacy Forum will publish on its web site a set of detailed consumer draft letters to help victims find and correct their records.

Conclusion

Medical identity theft is occurring right now. Victims are being harmed right now. Victims are experiencing a disturbing lack of recourse, lack of redress, and inability to recover from the crime due to structural, systemic problems built into the system.

There are not clear numerators for this crime, and in general, it appears that it is just now that the health care provider community is beginning to take some small preventive steps such as checking identification. However, this will not be enough to stop medical identity theft. This is a crime that is often committed by people who know they can make a lot of money from patients and the health care system, and these individuals are often running sophisticated schemes that are difficult to detect.

It is crucial to see the problem of medical identity theft clearly. This will take research and serious studies by both the government and the private sector. Survey instruments need to be designed anew, and need to include questions that will cull out and differentiate medical identity theft as a separate, unique crime so as to begin to better grasp its movements and characteristics.

Consumer education programs for victims of financial identity theft are well-refined; medical identity theft victims are in need of this same kind of refined information that is focused on the problems unique to medical identity theft, such as problems with medical files and amending records at insurers.

Some promising predictive technologies are in process now for health care fraud, and experts such as Malcolm Sparrow have created greater understanding of how to measure fraud. This learning needs to be applied to any iteration of the NHIN. To date, the NHIN has not been well-defined, and it may be over promising on what it can deliver. Going forward, the NHIN planning must include thoughtful and meaningful participation of

fraud experts, identity theft experts, technology and security experts who do not have a financial stake in the outcome, medical experts, privacy experts, and most importantly, people who are patients and who have been victims of this crime.

The victims who have been impacted by medical identity theft have to date been largely ignored, despite the serious consequences and harms they must face and deal with. It is now time to work diligently to create new pathways of help and recourse for these victims, who deserve to be heard and helped.

Credits

Report Author:

Pam Dixon, Executive Director, World Privacy Forum.

Contributor: Robert Gellman.

The author would like to thank the following individuals and organizations for their contributions to this report:

Malcolm K. Sparrow generously suggested the broad outline for this report. His comments about useful writing approaches to the complexity of fraud issues were greatly appreciated, and were useful.

Caitlin Tobin at the Federal Trade Commission performed miracles with FOIA requests.

Nils Frederickson at the Pennsylvania Attorney General's office

Michael Louks

Los Angeles FBI Health Care Fraud Unit

Chip Yost

Howard Goldblatt

Mike Ingram, California Department of Insurance SIU Bureau Chief

David Burnham at Transactional Records Access Clearinghouse (TRAC)

Connie Woodhead

Louis Sacaccio

Carolyn Pennington and Marie Whelan at the University of Connecticut

Linda Boak

For More Information:

PDF version of full report is located at
<http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf>

For updates to this report and other documents related to the report, see the World Privacy Forum's Medical Identity Theft page at
<http://www.worldprivacyforum.org/medicalidentitytheft.html>

For More Information Contact:

World Privacy Forum
www.worldprivacyforum.org
info2006@worldprivacyforum.org
+1 760.436.2489

The World Privacy Forum is a 501 (C) (3) non-profit, tax-exempt organization. Its focus is on public interest research and consumer education relating to privacy topics.

Version 1.4.1
May 8 2006