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.

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.

This document is the Executive Summary of the report

For More Information About This Report

Report Author:

Pam Dixon, Executive Director, World Privacy Forum.

Contributor: Robert Gellman. For a list of other contributors see Credits section in full report.

For updates and the complete report:

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 the full report see:
<http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf>

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.

V1.2