Anna Winkowski
Med Inf 407-Research Paper
December 5, 2008

Medical Identity Theft: What are we doing to protect the victims?

On April 27, 2004, President Bush signed Executive Order 13335, making it mandatory for all Americans to have electronic medical records or electronic health records within ten years (Dixon, 2008). The Office of the National Coordinator for Health and Information Technology was then created to oversee the nationwide adoption of health information technology and to ensure that this translates into significant improvement of quality and efficiency of care. The goal is to have medical files that could easily be accessible by hospitals, insurers, physicians and other ancillary providers no matter where the patient is. Appropriate treatment would be rendered as the health care provider would have immediate access to the patient's medical history.

On October 6, 2005, the Department of Health and Human Services (HHS) awarded a $3.3 million contract to the American National Standards Institute to organize the Health Information Technology Standards Panel which would be responsible in developing, creating and identifying a process that would support the compatibility among the different electronic health records software. The HHS also awarded $2.7 million to the Certification Commission for Health Information Technology to create the criteria and assessment tools in certifying electronic health records and framework or networks in which they operate. Lastly, the HHS awarded $11.5 million to RTI International, a not-for-profit corporation, to address the problem of interoperability of health information exchange resulting from varying levels of business policies and state laws affecting the privacy and security of health records (Dixon, 2008).

On May 23, 2006, the HHS announced that 22 states have signed subcontracts with RTI International, to focus on privacy and security questions that could affect the health information exchange (Dixon, 2008). Among the 22 states are: Alaska, Arkansas, Colorado, Iowa, Illinois, Indiana, Kentucky, Massachusetts, Maine, Michigan, Minnesota, Mississippi, North Carolina, New York, Ohio, Oklahoma, Rhode Island, Utah, Washington, Wisconsin, West Virginia, and Wyoming. Other states were expected to sign up in the coming weeks bringing the total number of states, expected to develop unified solutions in dealing with the barriers for health information exchange.

On September 28, 2007, the HHS announced that they have awarded contracts in the sum of $22.5 million to nine health information exchanges to pilot the Nationwide Health Information Network (NHIN) (Dixon, 2008). The following organizations would test and demonstrate the exchange of health information between physicians, patients and other health care providers:

- CareSpark – Tricities region of Eastern Tennessee and Southwestern Virginia
- Delaware Health Information Network – Delaware
- Indiana University – Indianapolis Metroplex
- Long Beach Network for Health – Long Beach and Los Angeles, California
- Lovelace Clinic Foundation – New Mexico
- MedVirginia – Central Virginia
- New York eHealth Collaborative – New York
- North Carolina Healthcare Information and Communications Alliance, Inc. – North Carolina
- West Virginia Health Information Network – West Virginia

The HHS believes that this pilot would bring the nation closer to a health care IT program which would improve the quality and efficiency of health care delivery, as well as improve disease prevention.

In June 2008, the Office of the National Coordinator for Health IT awarded a $450,000 contract to Booz Allen Hamilton to produce a report as to the extent of medical identity theft.

On December 15-16, 2008, the NHIN will conduct their 5th Annual Forum in Washington D.C., to present their progress report on the NHIN trial implementations. The Forum will highlight the experiences and lessons learned from the pilot study to enable interoperability of data exchange among organizations, protect exchanged information by developing trust agreements among NHIN participants and preparing for the roll out through lessons learned from the experience (Dixon, 2008).

Critics of the NHIN have expressed their concern over the network's ability to store substantial amount of personal information which an identity theft could easily gain illegal access to and result in the newest form of identity theft called medical identity theft.

Identity Theft

Identity Theft is the deliberate stealing of someone else's identity in order to obtain services, purchase items or steal money from the victim's existing accounts. According to Bob Young (2007), there are five types of identity theft:

- **Credit Card Theft** is when somebody steals your credit card information and uses that information to make purchases under your name. The perpetrator may even use your information to apply for other credit cards.

- **Driver's License Theft** is when somebody steals your driver's license information and commits various driving or traffic violations.
- **Social Security Number Theft** is when somebody steals your Social Security Number to create a whole new identity. This will allow the person to create a new account, apply for loans or obtain Social Security benefits
- **Criminal Identity Theft** is when the offender uses a false identity to commit a crime.
- **Medical Identity Theft** is when a person uses your personal information to obtain costly medical services. As a result, the criminal's health information is now included in your health information, which could prove deadly.

Although Credit Card Theft is the most common form of identity theft, Medical Identity Theft is now growing rapidly (Young, 2007) (Johnson, 2007). According to the World Privacy Forum (2006), the number of Americans identifying themselves as victims of medical identity theft had nearly tripled in just four years, to more than a quarter million in 2005.

Reasons behind Medical Identity Theft

There are several reasons a patient's medical identity would be targeted by criminals:

- **Obtain controlled substances**-health care workers with access to personal information might use the victim's identity to obtain prescription drugs to sell, or to support their own addiction. Pharmacists might bill the victim's plan for narcotics. Prescriptions might be called in by a nurse who picks it up themselves ((Johnson, 2007).

- **File false claims**-usually done by a health care professional who is familiar with the insurance billing system. Stolen patients information are used to file fake treatment claims to the policies of honest members (Johnson, 2007).
- **Receive free medical treatment**-people who are either unable to pay for their own health coverage or are here illegally, will use the victim's identity to receive free medical care with the victim's policy getting the claims (Johnson, 2007).

With over 47 million uninsured in the United States, Medical Identity Theft is a lucrative way for criminal elements to make some money. Until a few years ago, medical identity theft was believed to be the work of solo individuals who pretended to be someone else in order to receive medical care. Usually medical identity theft is an inside job committed by employees of the health care facility and resold on the black market. Criminals may also hack into a medical database or break into health care facilities. Nowadays, a disturbing trend is emerging: organized crimes, uncovered in California, Florida and New York, are getting involved in medical identity theft. Prosecutors revealed that these criminal organizations buy health care centers, steal the patients' information to file false insurance claims, then close the health care centers down before anybody notices their illegal activity (Johnson, 2007).

The Victims of Medical Identity Theft

There are several victims of medical identity theft (Theft, 2008). The primary victim is the **patient**, a potential patient, a health care consumer or a health plan member. Individuals with developmental or learning disabilities, minors, newborns, the elderly, patients whose information is in public registries and even the recently deceased are targeted. An individual may not know that they are the victim of medical

identity theft until much later, when they begin to receive questionable bills. Those who report it to the police may find the crime considered as a property theft and not a high priority for their limited resources (Theft, 2008).

Aside from questionable bills, the primary victim is faced with the emotional trauma of dealing with the loss of personal health information, whether deliberate or accidental. Patients will feel violated and unsafe even in their own home.

The secondary victim would be the **health plan and the health care providers** (Theft, 2008). It may be necessary for a health care provider to write off all of its health care expenses pertaining to the treatment of the identity thief. Smaller hospital organizations and small-time physician practice clinics will be greatly affected by the write off since they cannot bill the patient/victim. The provider may also have difficulty rescinding claims made prior to the discovery of the crime. In addition, significant expenses may be incurred by the provider and the plan as they work with the victim to try to resolve the records and prevent further risk. The provider or plan unaware of the medical identity theft might also disclose erroneous information to others, or provide services or treatment inappropriate to the victim. As discussed later in this paper, the dissemination of erroneous information could potentially kill a patient.

Medical identity theft poses a significant impact on the **society** as well (Theft, 2008) (Staff, 2008). To offset write offs, private-pay patients may find themselves paying more to health care providers. Insurance rates will increase to offset losses incurred. Tax payers will have additional taxes to pay for government-provided benefits to offset the cost of undiscovered and unrecovered claims. Some government-sponsored services might be discontinued or reduced due to lack of funds resulting from

unrecovered claims. In addition, to cover for the investigation, prosecution, incarceration and enforcement involving medical identity theft, tax payers will have to pay for increased federal and state law enforcement services.

Identity Theft Statistics

Below is the 2008 Data Breach Statistics as reported by the Identity Theft Resource Center (ITRC), a not-for-profit organization, whose focus is the understanding and prevention of medical identity theft. This report was accurate as of November 13, 2008:

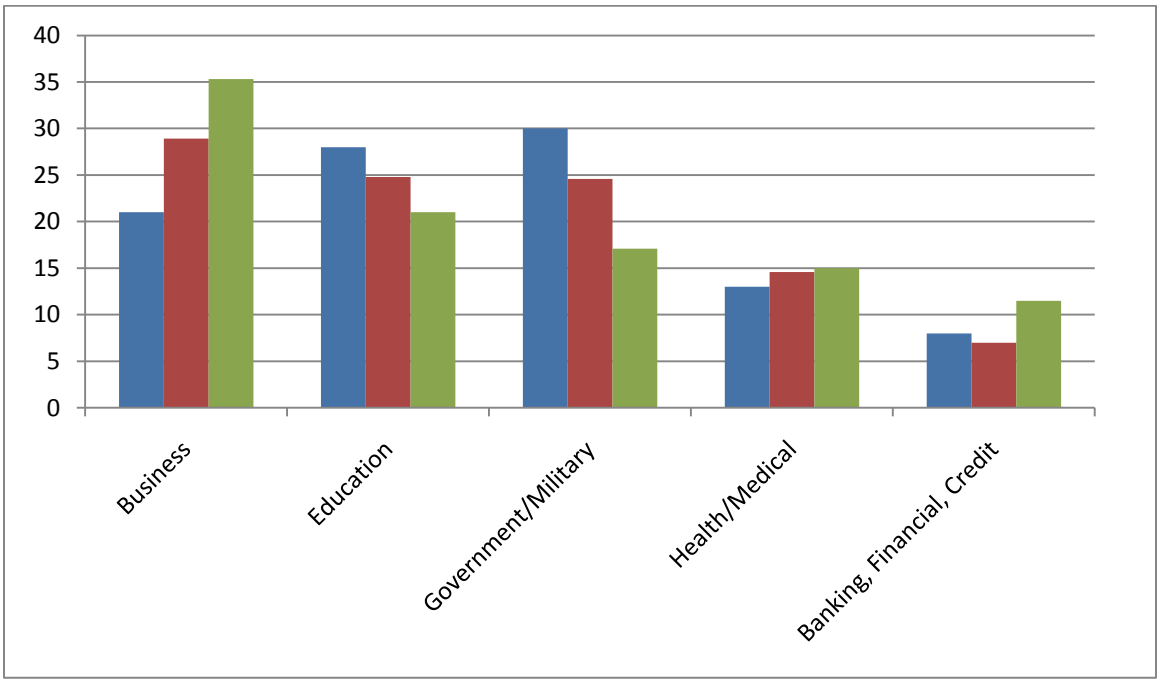


Figure 1 Source: Identity Theft Resource Center 2008

Although Business Identity Theft still leads with 35.3%, Medical Identity Theft is emerging as one of the crimes to watch with 15% of the breaches to date.

Identity Theft Sources

The ITRC further identified the how personal identities are stolen (Staff, 2008):

Insider Theft (stolen by someone inside the company):

2008 - 15.8% 2007 - 6.0%

Data on the Move (laptop, thumb drive, PDA, etc.):

2008 - 20.2% 2007 - 27.8%

Subcontractor (stolen or lost by a second party):

2008 - 13.5% 2007 - 11.4%

Hacking (stolen by someone outside of the company):

2008 - 11.7% 2007 - 14.1%

Accidental Exposure (inadvertent Internet/Web posting):

2008 - 15.2% 2007 - 20.2%

The above data shows how thieves are increasingly aware of the monetary value of personal information. Because of electronic medical records, an individual's personal information is easily accessible for those with malicious intent. It should also be noted that as the cases of accidental exposure, hacking and even data on the move has dropped, the cases of insider theft has more than doubled. This goes to show that as the economy worsens, more people are willing to find a way to make easy money.

Effects of Medical Identity Theft

Medical identity theft can be fatal. A person impersonating the victim could end up in the emergency room and identified as having a different blood type (Johnson, 2007). If the victim ends up in a serious accident and is taken to the same hospital, he could easily end up getting transfused with the wrong blood. The victim might also be given a medication he is allergic to or not given the medication needed because the impersonator who used the victim's identity in an earlier admission is allergic to that

particular medication. When a patient's information is stolen and used inappropriately and without consent, this could result in false claims, false research data, false public health reports and theft of medical services. The victim's health records will be corrupted which could result in health risks for the victim seeking treatment in the future. The effects of medical identity theft is not only limited to the health risks involved when the victim gets treated based on the erroneous record.

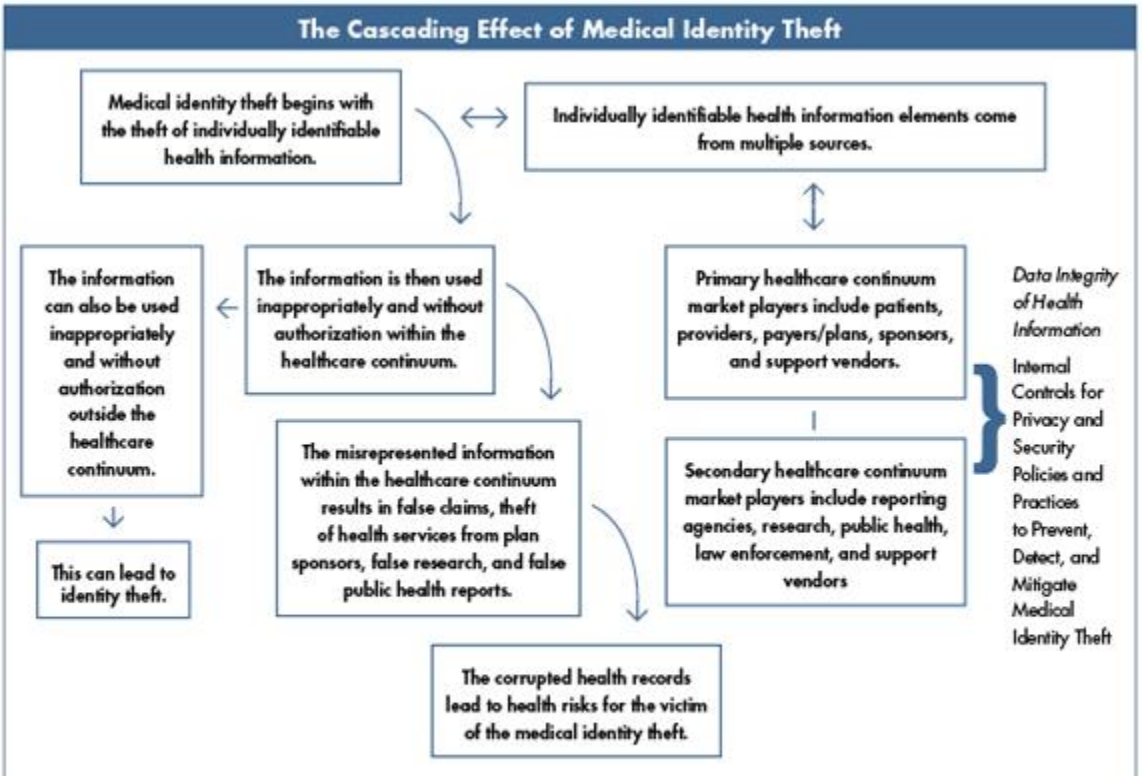
There are serious and long-term effects of medical identity theft which could take years before it gets corrected, if at all (Johnson, 2007). This does not include the mental and psychological stress that such crime could do to a person. The following effects are:

- **Damaged credit**-with the criminals racking up large bills under the victim's name without paying, the victim's credit could be ruined. Bill collectors may go after the victim, loans and mortgages will be turned down, and the victim will be charged with higher lending costs. Even worse, the victim might lose their job as employers check their employees' credit history. Victims applying for a new job may never get hired if their credit history is bad.
- **Forfeiture of health coverage**-false insurance claims can use up the victim's health policy limits leaving the victim with no coverage in a medical emergency or when the victim needs an operation or treatment.
- **Erroneous medical record**-as mentioned earlier, the impersonator's treatment history could end up in the victim's record which could include the wrong blood type, the wrong medication the victim is allergic to and even the wrong diagnoses such as mental illness or HIV.

- **Legal troubles**-the victim may have to hire a lawyer to fend off enforcement agencies that might take away the children especially if the impersonator is a drug addict. The victim may also need a lawyer to prove their innocence in criminal cases such as murder or theft, which was actually committed by the impersonator.
- **More expensive health premiums**-health premiums will be higher resulting from false insurance claims filed against the victim's health policy.

Cascading Effects of Medical Identity Theft

To further illustrate the effects of medical identity theft, the American Health Information Management Association (2007) included the flow chart below in their article "Mitigating Medical Identity Theft."



The effects of medical identity theft cascade throughout the healthcare continuum. Beyond being used to submit false claims, false data make their way into oversight agency databases, skewing public health findings. Ultimately, corrupted data in the victim's medical record may place the individual at risk in future treatment.

Economics of Medical Identity Theft

According to the AHIMA (2008), the street value of a stolen Social Security number is $1 per identity, while the price of stolen medical identity information is $50 per identity. At the Cleveland Clinic in Weston, Florida, an office coordinator stole the medical identity of more than 1,100 patients and sold it for $5 to $10 per patient. The records were then used to file false Medicare claims with reimbursement totaling more than $7 million. In his article The Coming Pandemic, Michael Friedenberg (2006), stated that it takes 600 hours, to restore a stolen identity. Companies spend an average of 1600 work hours per incident at a cost of $40,000 to $92,000 per victim, to clean up the mess. The FTC estimates that medical identity theft may cost the U.S. economy $468 million per year, a significant amount of money for a crime that could easily ruin the lives of the victims (Freidenberg, 2006).

Medical Identity Theft: What is being done?

Unfortunately, Medical Identity Theft is the most difficult identity theft to fix due to victims having limited recourse (Johnson, 2007). It leaves a trail of erroneous information which could haunt the victim for years since it is almost impossible to trace where the record have been distributed across networks of medical providers, insurers and government agencies. The Health Insurance Portability and Accountability Act of 1996 or HIPAA, requires health care providers and insurers to allow an individual to access their own medical records and to provide a copy of the privacy practices. If the records are not correct, HIPAA gives providers and insurers 90 days to respond to your complaints. If the health care provider does not agree, they do not have to do anything. In addition, HIPAA does not require the health care providers to remove incorrect

information in order to preserve a paper trail. HIPAA offers minimal support in resolving medical identity theft (Andrews, 2008).

It is often difficult for medical identity theft victims to find out whom, if any, to call for help. Because in some situation, the people they call from help may be the one responsible for the crime. In addition, financial identity theft is rarely a focus in the medical world with only a few familiar with the complexities in helping victims with error report problems. On the other hand, financial identity theft experts are not familiar with the HIPAA rule or the complex nature of medical care treatment and payment systems.

It is very important for medical identity theft victims to know what their options are. The laws that were designed to protect patient medical privacy are the same ones that are preventing the victims from viewing their charts and correcting erroneous entry.

World Privacy Forum

The World Privacy Forum, founded in 2003, is a non-profit, non-partisan 501 (C) (3) public interest research group, with emphasis on conducting in-depth research analysis, and consumer education in the area of privacy. Among the areas of great interest for the Forum are health care, technology and the financial sector. The World Privacy Forum's researches have been groundbreaking and trendsetting. It identified medical identity theft as a new area of concern (Dixon, 2008).

The World Privacy Forum created the Red Flag Rules Guidelines which provide suggestions on how health care providers can identify medical identity theft from their dealings with patients. The sensible health care (Gage, 2008)providers are advised to be on the lookout for signs that could potentially detect that patients are victims of medical identity theft:

- A complaint or question from a patient based on the patient's receipt of:
    - A bill for another individual
    - A bill for a product or service that the patient denies receiving
    - A bill from a health care provider that the patient never patronized
    - A notice of insurance (or Explanation of Benefits) for health services never received
- Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient
- A complaint or question from a patient about the receipt of a collection notice from a bill collector
- A patient or insurance company report that coverage for legitimate hospital stay is denied because the insurance benefits have been depleted or a lifetime cap has been reached
- A complaint or question from a patient about information added to a credit report by a health care provider or insurer
- A dispute of a bill by a patient who claims to be the victim of any type of identity theft
- A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance
- A notice or inquiry from an insurance fraud investigator for a private insurance company or a law enforcement agency

The World Privacy Forum recognized that it is extremely difficult for victims to correct their records once identity theft as occurred. As a result, the World Privacy

Forum offers these recommendations on what people should be allowed to do when they are victims of medical identity theft:

- 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.
- Victims of medical identity theft 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.
- Notification of medical data breaches to consumers has the potential to save lives, protect health, and prevent losses.
- A National Health Information Network should be established using comprehensive risk assessments focused on preventing medical identity theft while protecting patient privacy.

Protecting Against Medical Identity Theft

The American Health Information Management Association or AHIMA recommends that patients observe the following actions to prevent medical identity theft:

- Sharing personal and health insurance information only with trusted providers.
- Monitoring the explanation of benefits received from insurers and obtaining a summary each year of all the benefits paid in the patient's or guarantor's name.
- Contacting the insurer and provider about charges for care that was not received, even when there is no money owed.

- Maintaining copies of healthcare records.
- Checking personal credit history for medical liens.
- Demanding that providers and insurance companies correct errors or append and amend medical records to alert a user to inappropriate content.
- Questioning “free” medical services or treatments (sometimes illicit entities use the lure of “free” services to obtain names and insurance information for use in fraudulent claim submissions). Individuals should always question what is being offered and who is paying the cost. If not satisfied with the answers, they should decline the offer.
- Protecting health insurance information. Individuals should safeguard insurance cards, explanation of benefits, and health plan correspondence in the same way they would safeguard credit cards.
- Refusing to provide insurance numbers to telephone marketers or door-to-door solicitors.

Legislation Against Medical Identity Theft

As the cases of medical identity theft are growing rapidly, it is quite notable that there is no single legislation addressing the problem. Each state addresses the issue of identity theft. However, only three states Arkansas, California and Delaware addressed the issue of medical identity theft.

- **California**. AB1298, or Confidentiality of Medical Information Act, which took effect on January 8, 2008, broadens California’s data-breach notification law to also include unencrypted medical records, information regarding a person’s mental and physical conditions, medical treatments and diagnosis (Gage, 2008)

Basically, the law requires health establishments to notify patients in the event there is a breach of their medical record. California's data breach law, SB1386, initially covered financial records only. Violations could result in a civil action for compensatory or punitive damages. If an economic loss or a personal injury to a patient is attributed to the violation, it is punishable as a misdemeanor.

- **Arkansas**. On February 2, 2007, the Arkansas House approved higher penalties for anybody who uses someone else's identity to avoid criminal prosecution, harass another person or attempt to receive a good, service, property or medical information of someone else. In a 96-0 vote, the new bill would allow the court to impose on anyone convicted of the crime, to pay compensation to their victims.
- **Delaware**. On April 25, 2007, the 144th General Assembly amended Title 11 of the Delaware Code relating to identity theft. Individuals caught purchasing narcotics under someone else's identity will be arrested by law enforcement officers as per House Bill 117.
- **Illinois**. Unfortunately, out of the 1448 Senate Bills pertaining to identity theft that were reviewed, not a single one mentioned medical identity theft.

However, the United States Senate, over the last year, has started to address the issue of medical identity theft.

- **H.R. 3800** which encourages the adoption of nationwide interoperable health information technology also gives individuals the right to review and request a copy of their protected health information stored in electronic format. Introduced in October 10, 2007, this resolution also requires providers to notify individuals whose identifiable health information was accidentally disclosed.

- **H.R. 5442**, introduced February 14, 2008, allows individuals access to their own health information, enforce criminal and civil punishment to those who use personal health information without prior permission and to safeguard the personal privacy, security and confidentiality of health related personal information.

Marcy Wilder, a partner at Hogan and Hartson predicted that legislation in 2009 will be passed by Congress which will strengthen federal law to combat medical identity theft (Pulley, 2008). As of now, HIPAA and the states' data breach notification laws are the strongest legal protection against medical identity theft.

Patient Credit Score

A hospital risk tool is being developed by Healthcare Analytics to help determine a patient's ability to pay his medical bills. Tentatively known as "MedFICO Score," it will be similar to credit scores (Sullivan, 2008). Healthcare Analytics has been collecting payment information from hospitals nationwide. The data will then be used to analyze a patient's ability to pay future bills. Patients who failed to pay their medical bills in the past are more likely to repeat the same pattern in the future and will therefore be assigned a lower MedFICO score.

However, Pam Dixon from World Privacy Forum expressed concern that patients with low MedFICO score might not receive the treatment they need at the time when they need it. Dixon is also concerned that victims of medical identity theft who would most likely end up with low MedFICO score might be denied treatment as a result of the low score which the victims had nothing to do with. Tim Hurley, a Healthcare Analytics spokesman, downplays the concern stating that the MedFICO score is still in

development and is therefore not ready for hospital use. Hurley also disputed the claims that patients would be denied treatment as a result of their MedFICO score. According to Hurley, hospitals would only use the MedFICO score to determine the patient's ability to pay their medical bills after they receive treatment (Sullivan, 2008). This way, hospitals would know what type of payment options they could offer the patients. Some hospitals might even write off the medical bills as a charity case instead of having delinquent accounts sitting in their accounts receivables.

Comparison of Victim's Rights

To illustrate the uphill battle that victims of medical identity theft face when trying to correct the issue, one has to look at the table below to realize that it is easier for financial identity theft victims to clear their records and correct their credit reports:

Victim's Rights	Financial Identity Theft	Medical Identity Theft
See and correct errors in credit reports	Yes	No. Victims do not have the blanket right to correct errors on their files. Some victims have not been allowed to view the compromised files
File fraud alerts	Yes	Yes. However medical identity theft does not always show through traditional financial reports
Obtain documents or information relating to transactions involving their personal information	Yes	No.
Right to prevent consumer reporting agencies (such as credit bureaus) from reporting information resulting from identity theft	Yes	No

Table 1 Source: Medical identity theft turns patients into victims, 2008

Booz Allen Hamilton

As mentioned earlier, Booz Allen Hamilton was awarded a contract by HHS to determine the extent of medical identity theft. They conducted an Environmental Scan to better understand and address the issues concerning medical identity theft which they believe would not only have an absolute and damaging impact on consumers and health care providers in the health care system but compromise the reliability, accuracy and efficiency of the health information exchange (Booz Allen Hamilton, 2008).

They conducted 34 interviews between the months of June and September 2008, asking questions ranging from experience and knowledge of medical identity theft, to their insight on the scope of the problem. The interviewees were also asked if they are aware of any existing methods that have proven effective in fighting medical identity theft, or if they have any suggestions on the role health IT could have in preventing, detecting and remediating medical identity theft (Booz Allen Hamilton, 2008).

The Environmental Scan as conducted by Booz Allen Hamilton was able to identify several possible responses to medical identity theft. Although the extent and magnitude of medical identity theft has not been accurately estimated, the interviewees agreed that the lack of knowledge limits their ability to select appropriate responses to the problem. The interviews conducted were able to identify several methods to address medical identity theft, already used by some organizations. These methods may need to be integrated into a widespread solution, still in its early stages of development. Opportunities and risks abound as sizeable networks are needed to support widespread electronic health information exchange. Health IT has an important role in developing an effective tool in preventing, detecting and correcting medical identity theft.

Conclusion

Although AHIMA and the World Privacy Forum have made their recommendations on appropriate responses to reduce or eliminate the harmful effects of medical identity theft, these responses are still in its early stages of development and are not as robust as that of the financial industry's response to identity fraud. Victims of medical identity theft have limited recourse, if any; in correcting their records once the crime is committed. Current responses are aimed at punishing the medical identity theft perpetrators and providing financial restitution to the victims. However, little has been written about what the victims could do to return their records to their previous state before the breach occurred. Although the HIPAA Privacy Rule allows victims to request removal of inappropriately inserted information from their records, under the same HIPAA Privacy Rule, providers may refuse the request, though some may note in the health records that a request has been made. It is therefore of utmost importance to revisit the HIPAA Privacy Rule and make the necessary changes so victims of medical identity theft are able to access their records and make the corrections so their care will not be compromised by corrupted health records. Legislations are also needed not only to punish the medical identity theft perpetrators but also to ensure that victims are able to reduce or eliminate the damaging effects of medical identity theft.

References:

Andrews, M. (2008, February 29). *Living Well*. Retrieved October 1, 2008, from health.usnews.com: http://health.usnews.com/articles/health/living-well-usn/2008/02/29/medical-identity-theft-turns-patients-into-victims.html?PageNr=1

Assembly, D. G. (2007, April 4). *Bill Tracking*. Retrieved October 1, 2008, from State of Delaware: http://legis.delaware.gov/LIS/lis144.nsf/2bede841c6272c888025698400433a04/86be717ddd6c67b8852572ad0066c769?OpenDocument

Booz Allen Hamilton. (2008). *Medical Identity Theft Environmental Scan.* Maryland: Booz Allen Hamilton.

deMillo, A. (2007, February 4). House passes increased penalties for identity theft. Little Rock, Arkansas, USA.

Department of Health and Human Services. (2007, April 9). *Healthy People 2010*. Retrieved July 12, 2008, from Department of Health and Human Services Website: http://www.healthypeople.gov/data/midcourse/html/focusareas/FA06TOC.htm

Dixon, P. (2008, October 3). *World Privacy Forum*. Retrieved November 10, 2008, from http://www.worldprivacyforum.org/NHIN_timeline.html

Freidenberg. (2006). The Coming Pandemic. *CIO Magazine* .

Gage, D. (2008, January 4). *California data-breach law now covers medical information*. Retrieved October 1, 2008, from San 1Francisco Chronicle: http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/01/04/BUR6U9000.DTL&type=printable

Johnson, A. T. (2007, April 4). *More doctors, insurers asking, 'Who are you?'*. Retrieved October 1, 2008, from NBC News: http://www.msnbc.msn.com/id/17048911/

Pulley, J. (2008, October 16). *Experts predict federal law on medical ID theft*. Retrieved October 18, 2008, from Government Health IT: http://www.govhealthit.com/online/news/350621-1.html

Staff, I. T. (2008, July 17). *Identity Theft News*. Retrieved October 1, 2008, from http://idtheftmostwanted.org/ITRC%20Breach%20Stats%20Report%202008.pdf

Sullivan, B. (2008, January 18). *The doctor will see your credit now*. Retrieved October 1, 2008, from The Red Tape Chronicles: http://redtape.msnbc.com/2008/01/the-doctor-wi-1.html

Theft, A. e.-H. (2008, July). Mitigating Medical Identity Theft. *Journal of AHIMA* , 63-69.

Young, B. (2007, July 25). *Young Money*. Retrieved October 1, 2008, from Youngmoney.com: http://www.youngmoney.com/shopping/consumer_fraud/133