Identity Theft That Can Kill You

Kirsten A. Davenport, J.D., LL.M. Candidate

"Identity theft is one of the fastest growing, non-violent crimes in America, and thousands of people and services are defrauded each year, causing millions of lost dollars and greatly increased insurance costs."[1] The Federal Trade Commission estimates that in a five-year period prior to early 2003, in the United States alone, there were 27.3 million reported cases of identity theft.[2]

Everyone is familiar with identity theft, but a new form of identity theft is potentially fatal: medical identity theft. Medical identity theft is when a person uses another person's identity, without their knowledge, to obtain medical care or services. It can be fatal because the identity thief's medical information, such as diagnosis, blood type and/or drug allergies, becomes intertwined in the victim's medical information. The victim of medical identity theft generally remains unaware of the violation until they receive bills for services they did not receive or an "explanation of benefits" from their insurance provider listing services not received by the insured, or they are denied coverage for medical care because their benefits have been exhausted by the thief.

A recent example of medical identity theft involved a woman who received demands for payment of hospital bills for the amputation of her left foot, yet never had either of her feet amputated.[3] In response, she sent the collection agency notarized pictures of her two, still attached feet, and refused to pay the bills.[4] Though she made great efforts to remove the imposter's medical information from her medical information, during a subsequent hospitalization, she was asked by a health care professional what she was taking for her diabetes – a condition of the imposter rather than her own.[5]

Efforts to remediate the incorrect records will be met with several hurdles. While victims of traditional identity theft have recourse through credit bureaus, fraud alerts and rights to obtain documentation pertaining to the theft, victims of medical identity theft are limited in their recourse due to the inherent privacy in such records. And HIPAA does nothing to help the situation.

"The HIPAA Privacy Rule standards address the use and disclosure of individuals' health information ("protected health information") by organizations subject to the Privacy Rule ("covered entities") as well as standards for individuals' privacy rights to understand and control how their health information is used."[6] A primary goal of HIPAA is to "assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect

---

1 Commonwealth of Pennsylvania v. Johnette O. Young, 895 A.2d 40, 43 2006 Pa. Super Ct. 46 (2006)
2 Daly v. Metropolitan Life Ins. Co., 782 N.Y.S.2d 530, 535 (2004) (citation omitted).
3 Joseph Menn, *ID Theft Infects Medical Records*, L.A. TIMES, Sept. 25, 2006
4 *Id.*
5 *Id*.
6 Office for Civil Rights, *Summary of the HIPAA Privacy Rule*, http://www.hhs.gov/ocr/privacysummary.pdf (last viewed Oct. 15, 2006).

the public's health and well being."[7] But this "flow" of information does not necessarily benefit the patient. Because of HIPAA, patients do not have the kind of access or control necessary to purge their records of an imposter's medical information.

The goal of the victim of medical identity theft will obviously be to amend their medical records to remove information that may affect their future insurance coverage and medical treatment. Under most circumstances, individuals have the right to review and obtain a copy of their protected health information in a covered entity's designated record set, but this access may be denied if the protected health information makes reference to another person.[8] The privacy rule that keeps a patient's records private, also keeps the imposter's records private, and health care providers can refuse a patient access to his own records based on the imposter's privacy rights. A patient can request a review of the provider's refusal of access in this situation, but that review is performed by a licensed health care professional designated by the provider denying access.[9] Though providers are required to provide the patient portions of their records that are not specifically excluded for containing an imposter's information, situations may arise where the victim's records and the imposter's records are so intertwined that they are not able to be segregated.

If the victim is able to obtain access to his or her records, he or she has a right to request amendment of any information that is inaccurate or incomplete.[10] But again, the request for amendment can be denied on the basis that the victim is requesting amendment of another person's information.[11] Further, providers are not required to amend information that was received from another source and that they did not actually create.[12] With impediments such as these, it may be impossible for a victim to erase false entries from their medical or insurance record."[13]

An exacerbating factor is the dissemination of health information among medical providers, insurers, pharmacies and billing agencies. Even if the victim is able to clear his/her record from one provider, the imposter's information will likely have already been sent to numerous other entities through electronic means. Despite HIPAA's constraints on the use and disclosure of information, health care providers can disclose protected health information without the patient's consent for many purposes including treatment related activities, payment related activities, healthcare operations, or public policy activities.

To assist in the identification of providers or entities that have received the imposter's information, patients have a right to receive an accounting of the disclosures of their protected health information (or the imposter's information in this situation). Providers

---

[7] *Id*.
[8] 45 C.F.R. § 164.524(a)(3)(ii).
[9] 45 C.F.R. § 164.524(a)(4).
[10] 45 C.F.R. § 164.526(a)(1).
[11] 45 C.F.R. § 164.526(a)(2).
[12] 45 C.F.R. § 164.526(a)(2)(i).
[13] PAM DIXON, MEDICAL IDENTITY THEFT: THE INFORMATION CRIME THAT CAN KILL YOU (2006) http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf (last viewed on Oct. 15, 2006).

are obligated to keep track of what information was disclosed, when it was disclosed and to whom it was disclosed. This is a good starting point for the victim, but there are many exceptions to this obligation. Providers are not obligated to track disclosures, for example, for billing and treatment.[14]

In 2003, a detailed report on medical identity theft was published by The World Privacy Forum, a non-profit public interest research and consumer education group. The Forum proposed certain changes to HIPAA to assist patients in the remediation of their records. Suggestions include expanding the provider's requirement of tracking disclosures, and expanding the victim's rights to amend and delete errors in their information that are due to identity theft and fraud.[15] The Forum's suggestions for the victim include requesting that the provider create a separate record if they are not willing to totally remove the incorrect information; if the entity agrees to amend the information, insist that they notify other entities to whom the information has been distributed; make a police report; review closely all explanations of benefits received from insurers; and keep copies of medical records.[16]

In this age of information, an insightful judge noted

> I know that the notes from the visit to my doctor's office may be transcribed in some overseas country under an out-sourcing contract by a person who couldn't care less about my privacy. I know that there are all sorts of businesses that have records of what medications I take and why. I know that information taken from my blood sample may wind up in databases and be put to uses that the boilerplate on the sheaf of papers I sign to get medical treatment doesn't even begin to disclose. I know that my insurance companies and employer know more about me than does my mother. I know that many aspects of my life are available on the Internet. Even a black box in my car--or event data recorder as they are called--is ready and willing to spill the beans on my driving habits, if I have an event--and I really trusted that car, too.[17]

The dissemination of health care information among health care entities can lead to a quagmire for victims of medical identity theft. With vigilance and perseverance, victims may be able to clear their records, but in an abundance of caution should always check the provider's records before seeking treatment.

---

[14] 45 C.F.R. §164.506(c).
[15] Dixon, supra note 13 at 15.
[16] Dixon, supra note 13 at 53-54.
[17] State v. A Blue in Color 1993 Chevrolet Pickup, 328 Mont. 10, 116 (Nelson, J., concurring).