

# Medical Identity Theft: What You Should Know

## Information for Patients

### *What is medical identity theft?*

Medical identity theft is when someone's personal information is used, without permission, to get money, prescription medicines, or medical services. Examples: a person uses someone else's name and information to have a surgery, causing that person to be billed for the surgery; a group of criminals uses information stolen from a health clinic to bill the insurances of individuals for services that were not actually provided.

### *What kinds of problems can medical identity theft cause?*

Medical identity theft can cause a person to be billed for healthcare that they didn't receive, which can cost thousands of dollars. It can also involve the addition of false or incorrect information to a person's health records. This is dangerous because it could cause you to be treated incorrectly by a doctor, based on the false information.

### *How can I stop it?*

Medical identity theft can be hard to detect. The best thing you can do is pay attention to ALL documentation pertaining to your healthcare:

- Review all insurance statements and bills for accuracy.
- Request summaries each year of what your insurance(s) paid. If you see something wrong, like a medical device, treatment, or service that you did not receive, contact your insurer and your healthcare provider immediately.
- Review your credit report regularly. There may be collection notices for hospitals, medical labs, or other medical services listed if you are a victim of medical identity theft.
- It can be pricey, but you can request copies of your medical records to make sure the information is correct and that it is about you.
- Ask for a list (called an "Accounting of Disclosures") of who your medical information has been given to. It's not a perfect record, but could be helpful if you find out that something is wrong and needs to be corrected.
- Always notify your insurance company if you lose your insurance card.

### *What should I do if I'm a victim?*

If you suspect that you are a victim of medical identity theft, you may need to deal with both credit problems and incorrect information in your medical records. Use the following list to make sure you cover all your bases:

- Check insurance benefits paid to you in the last year.
- Check your credit report. If there are incorrect charges, you will need to contact the billing department of the provider who is billing you to explain that it is a case of identity theft.
- File a police report, and get a copy for yourself.
- Get a copy of your medical records, and mark any information that isn't about you. Speak with your provider about the best way to fix the information. (There's a link to a sample letter on the following page to help you with this).
- Get a list of disclosures of your medical record, so you know who else might have the incorrect information (insurances, providers, etc).
- Be sure to notify all of your providers of incorrect information in your medical records.

<b><i>Identity Theft Resources</i></b>	
<b>Identity Theft Resource Center</b> For state and local resources, help correcting medical records, and sample letters to use for requesting your health records	858-693-7935 <a href="http://www.idtheftcenter.org">www.idtheftcenter.org</a>
<b>Department of Health and Human Services</b> For help if you have problems accessing your medical records, or to file a complaint	800-368-1019 <a href="http://www.hhs.gov/ocr/hipaahowto.pdf">www.hhs.gov/ocr/hipaahowto.pdf</a> <a href="http://www.hhs.gov/ocr/hipaa/consumer_summary.pdf">www.hhs.gov/ocr/hipaa/consumer_summary.pdf</a>
<b>Fair Credit Billing Act</b> For help with removing incorrect debt	877-382-4357 <a href="http://www.ftc.gov/bcp/online/pubs/credit/fcb.htm">www.ftc.gov/bcp/online/pubs/credit/fcb.htm</a>
<b>World Privacy Forum</b> Tips to prevent medical identity theft	760.436.2489 <a href="http://www.worldprivacyforum.org/medidtheft_consumertips.html">www.worldprivacyforum.org/medidtheft_consumertips.html</a>
<b>Public Safety Canada</b> Information on identity theft	613-991-3301 <a href="http://www.ps-sp.gc.ca/prg/le/bs/report-en.asp">www.ps-sp.gc.ca/prg/le/bs/report-en.asp</a>
<b>Canada's Office of Consumer Affairs</b>	613-954-5031 <a href="http://www.ic.gc.ca/epic/site/oca-bc.nsf/en/ca01360e.html#medical">www.ic.gc.ca/epic/site/oca-bc.nsf/en/ca01360e.html#medical</a>
<b>To request a copy of your credit report</b>	800-685-1111 (U.S. and CAN) <a href="http://www.equifax.com">www.equifax.com</a> (U.S.) <a href="http://www.equifax.com/home/en_ca">www.equifax.com/home/en_ca</a> (CAN)  888-397-3742 (U.S.) <a href="http://www.experian.com">www.experian.com</a>  888-826-1718 (CAN) <a href="http://www.experian.com/intl/canada.html">www.experian.com/intl/canada.html</a>  877-322-8228 (U.S.) <a href="http://www.transunion.com">www.transunion.com</a>  800-663-9980 (CAN [outside Quebec]) 877-713-3393 (CAN [Quebec]) <a href="http://www.transunion.ca">www.transunion.ca</a>

## Medical Identity Theft

### ***Introduction***

Medical identity theft involves the use of an individual's personal information, without that person's knowledge or consent, to collect money, prescription drugs, medical goods, or health services.<sup>1</sup> It's not only potentially damaging financially, but it can also be dangerous to a person's health. Medical identity theft can result in fictitious information and wrong histories and diagnoses being included in patients' charts and records.<sup>1</sup> The incidence of medical identity theft is thought to be on the rise. It's speculated that up to half a million people have been victims.<sup>1</sup> Although anyone, from neonates to the elderly, could be victimized, those who frequently access the healthcare system are most vulnerable.<sup>2</sup> The patient handout included with this document will help make patients aware of medical identity theft, and give them the resources to prevent and rectify medical identity theft.

### ***How Does It Happen?***

Medical identity theft can result from something as simple as one person using another person's social security number (or social insurance number in Canada) and name for a hospital admission, procedure, or treatment. It can also happen when corrupt healthcare workers and organized crime rings file false claims with insurance companies for procedures and treatments that never took place.<sup>1</sup>

Current evidence suggests that people with legitimate access to computer systems and/or patient data may often be the primary culprits in medical identity theft.<sup>3</sup> While much of the responsibility of preventing medical identity theft lies in the realm of health information systems, there are common sense steps that healthcare professionals can take to reduce opportunities.

### ***What Should Pharmacies Do?***

Lawsuits have been brought against pharmacies that have improperly disposed of confidential patient information in unsecured

dumpsters. This information included names and social security numbers of thousands of patients in several U.S. cities, and was certainly an opportunity for medical identity theft to occur.<sup>4</sup>

Some pharmacies have implemented strategies to prevent breach of private patient information. Some of these include special disposal of patients' old vials, locking of outdoor dumpsters, inspection of all trash to be sure that it doesn't contain private patient information, requiring all trash from the pharmacy be returned to company warehouse facilities for disposal, or shredding all trash that has private patient information. Regardless of the mechanism through which it is achieved, the goal is to be certain that personal information of patients is not disclosed to anyone other than the appropriate pharmacy staff.

Other precautions that are in place to protect patient information for HIPAA are also prudent. These include pointing computer screens away from public areas, and keeping discussions with or about patients as private as possible.

### ***What Should Prescribers Do?***

Prescribers should keep in mind the same goal as pharmacists, to protect private patient information from being accessed by anyone other than the appropriate healthcare professionals. Discard documents with private patient information in bins designated for confidential documents. If none are available, initiate their implementation.

There are reports of laptops with patient information being stolen from the homes and cars of physicians. Don't create this opportunity for thieves.<sup>3</sup> Keep patient charts closed when not in use, and remember to avoid leaving charts and patient information in unsecured or easily accessed areas. The black market value of a single medical record may be \$60 to \$70.<sup>5</sup>

Physicians can experience theft of their professional identities for the purpose of committing medical identity theft. Takeovers of clinics by crime rings and cases of imposters

*More . . .*

posing as physicians for the purpose of fraudulent billing are documented. There are reports of scams involving phone calls to physicians asking for sensitive identity information, like driver's license number, social security number, universal professional identification number, educational background, and birth date. The callers have represented themselves as Medicare audit or claims employees, Medicare fraud investigators, or employees of major insurance companies. It is noted that ethnic minorities may be specific targets of this activity.<sup>6</sup> Be aware of this and guard your personal and professional information.

### ***What Can Patients Do?***

Medical identity theft isn't easy to detect, so being vigilant and proactive is key. Once medical identity theft occurs, it can be challenging for victims to get copies of their medical records and to have the inaccurate information removed from their medical records. Unfortunately, HIPAA can inadvertently act as a barrier to achieving these things. For example, victims don't have the legal right to demand correction of medical information that was not created by their current provider or insurer.<sup>2</sup> In addition, a person's medical information may be disseminated to multiple entities, making it difficult to correct all erroneous information. Laws similar to those that help victims of financial identity theft are not in place for victims of medical identity theft.

Patients should always review the "Explanation of Benefits" sent to them by insurers. If anything is wrong, like charges for services, office visits, or medical equipment that wasn't received, the insurer and provider should be contacted.<sup>7</sup>

A list of benefits paid in a person's name should be proactively requested from insurers each year and reviewed for discrepancies, like services and goods that were not received. If any are found, the insurer and provider should be contacted.<sup>7</sup>

An "Accounting of Disclosures" should be requested yearly. This is a record of the disclosures of a person's health information made by healthcare providers or insurers. This information may be helpful in tracking where erroneous information, if it exists, may have been circulated.<sup>7</sup>

Keeping an eye on credit reports is important too. Victims of medical identity theft may have

collection notices for hospitals, medical labs, or other medical services on their reports.<sup>7</sup>

Individuals can request copies of their medical records, and keep their own personal copy. This can help a person detect discrepancies, and ensure that accurate information is available if medical identity theft occurs.<sup>7</sup> Patients may hear about websites that allow them to keep their own electronic personal health records (e.g., HealthVault, HealthFrame, YourMedChart, PersonalMD, etc). While these sites may offer a convenient way for patients to keep track of their health information, they are not always subject to HIPAA's protections.

For victims of identity theft, the main goals will be to correct both credit reports and medical records.

### ***Conclusion***

Medical identity theft is very complicated, dangerous, and damaging. It isn't easily identified by victims. It is a relatively new crime, and as such, safeguards against it might not be optimal with present systems and policies.

Despite the fact that much of the responsibility of protecting private patient information lies with health information systems, each healthcare professional must be aware of the risk, follow policies and procedures that are in place, and be vigilant of preventing opportunities for breaches.

Educating patients on ways to prevent and detect medical identity theft is important as well. Use our patient handout "Medical Identity Theft: What You Should Know" to provide patients with the information they need about this evolving crime.

---

*Users of this document are cautioned to use their own professional judgment and consult any other necessary or appropriate sources prior to making clinical judgments based on the content of this document. Our editors have researched the information with input from experts, government agencies, and national organizations. Information and Internet links in this article were current as of the date of publication.*

***Project Leader in preparation of this Detail-Document:*** Stacy A. Hester, R.Ph., BCPS, Assistant Editor

### ***References***

1. Griffin RM. The scary truth about medical identity theft. WebMD.com. [www.webmd.com/a-to-z-guides/features/scary-truth-medical-identity-theft](http://www.webmd.com/a-to-z-guides/features/scary-truth-medical-identity-theft). (Accessed November 7, 2007).

*More . . .*

2. Dixon P. Medical identity theft: the information crime that can kill you. World Privacy Forum. [www.worldprivacyforum.org/pdf/wpf\\_exsum\\_medidtheft2006.pdf](http://www.worldprivacyforum.org/pdf/wpf_exsum_medidtheft2006.pdf). (Accessed November 7, 2007).
3. Dixon P. World Privacy Forum speech. AHIMA National Convention General Session. Philadelphia, PA. October 9, 2007.
4. Anon. Indiana attorney general files charges against pharmacies. [www.wthr.com/Global/story.asp?S=7089029](http://www.wthr.com/Global/story.asp?S=7089029). (Accessed November 7, 2007).
5. Roop ES. Stealing you - medical identity theft. *Radiology Today*. [www.radiologytoday.net/archive/rt10232006p16.shtml](http://www.radiologytoday.net/archive/rt10232006p16.shtml). (Accessed November 7, 2007).
6. Vogt K. Physicians being targeted in identity theft scheme. *American Medical News*. [www.ama-assn.org/amednews/2005/01/31/bisd0131.htm](http://www.ama-assn.org/amednews/2005/01/31/bisd0131.htm). (Accessed November 7, 2007).
7. Anon. Medical identity theft: what to do if you are a victim (or are concerned about it). World Privacy Forum. [www.worldprivacyforum.org/medidtheft\\_consumertips.html](http://www.worldprivacyforum.org/medidtheft_consumertips.html). (Accessed November 7, 2007).

*Cite this Detail-Document as follows: Medical identity theft. Pharmacist's Letter/Prescriber's Letter 2007;23(12):231201.*

**PHARMACIST'S**  
**LETTER** 

*Evidence and Advice You Can Trust...*

**PRESCRIBER'S**  
**LETTER** 

3120 West March Lane, P.O. Box 8190, Stockton, CA 95208 ~ TEL (209) 472-2240 ~ FAX (209) 472-2249  
Copyright © 2007 by Therapeutic Research Center

Subscribers to *Pharmacist's Letter* and *Prescriber's Letter* can get *Detail-Documents*, like this one, on any topic covered in any issue by going to [www.pharmacistsletter.com](http://www.pharmacistsletter.com) or [www.prescribersletter.com](http://www.prescribersletter.com)