FTC FACTS for Consumers

Medical Identity Theft

Could identity thieves be using your personal and health insurance information to get medical treatment, prescription drugs or surgery? Could dishonest people working in a medical setting be using your information to submit false bills to insurance companies? Medical identity theft is a twist on traditional identity theft, which happens when someone steals your personal information. Like traditional identity theft, medical ID theft can affect your finances; but it also can take a toll on your health.

The Ill Effects of Medical Identity Theft

How would you know if your personal, health, or health insurance information has been compromised? According to the Federal Trade Commission (FTC), the nation's consumer protection agency, you may be a victim of medical identity theft if:

- you get a bill for medical services you didn't receive;
- a debt collector contacts you about medical debt you don't owe;
- you order a copy of your credit report and see medical collection notices you don't recognize;
- you try to make a legitimate insurance claim and your health plan says you've reached your limit on benefits; or
- you are denied insurance because your medical records show a condition you don't have.

Medical identity theft may change your medical and health insurance records: Every time a thief uses your identity to get care, a record is created with the imposter's medical information that could be mistaken for your medical information – say, a different blood type, an inaccurate history of drug or alcohol abuse, test results that aren't yours, or a diagnosis of an illness, allergy or condition you don't have. Any of these could lead to improper treatment, which in turn, could lead to injury, illness or worse.

An Ounce of Prevention

While there's no fool-proof way to avoid medical identity theft, the FTC says you can take a few steps to minimize your risk.

- **Verify a source before sharing information.** Don't give out personal or medical information on the phone or through the mail unless you've initiated the contact and you're sure you know who you're dealing with. Be wary of offers of "free" health services or products from providers who require you to give them your health plan ID number. Medical identity thieves may pose as employees of insurance companies, doctors' offices, clinics, pharmacies, and even government agencies to get people to reveal their personal information. Then, they use it to commit fraud, like submitting false claims for Medicare reimbursement.

- **Safeguard your medical and health insurance information.** If you keep copies of your medical or health insurance records, make sure they're secure, whether they're on paper in a desk drawer or electronic in a file online. Be on guard when you use the Internet, especially to access accounts or records related to your medical care or insurance. If you are asked to share sensitive personal information like your Social Security number, insurance account information or any details of your health or medical conditions on the Internet, ask why it's needed, how it will be kept safe, and whether it will be shared. Look for website privacy policies and read them: They should specify how site operators maintain the accuracy of the personal information they collect, as well as how they secure it, who has access to it, how they will use the information you provide, and whether they will share it with third parties. If you decide to share your information online, look for indicators that the site is secure, like a lock icon on the browser's status bar or a URL that begins "https:" (the "s" is for secure). Remember that email is not secure.

- **Treat your trash carefully.** To thwart a medical identity thief who may pick through your trash or recycling bins to capture your personal and medical information, shred your health insurance forms and prescription and physician statements. It's also a good idea to destroy the labels on your prescription bottles and packages before you throw them out.

Detecting Medical Identity Theft

Paying close attention to your medical, insurance and financial records can help you spot discrepancies and possible fraud.

- **Read the Explanation of Benefits (EOB) statement** that your health plan sends you after treatment. If you are a Medicare beneficiary, read the Medical Summary Notice. Make sure the claims paid match the care you received. Look for the name of the provider, the date of service, and the service provided. If there's a discrepancy, contact your health plan to report the problem.

- **Order a copy of your credit reports,** and review them carefully. Credit reports are full of information about you, including what accounts you have and whether you pay your bills in a timely way. The law requires each of three major nationwide credit reporting companies – Equifax, Experian and TransUnion – to give you a free copy of your credit report each year if you ask for it. Visit **www.AnnualCreditReport.com** or call 1-877-322-8228 to order your free credit reports each year, or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can download the form at **www.ftc.gov/freereports**.

Once you have your reports, look for inquiries from companies you didn't contact, accounts you didn't open, and debts on your accounts that you can't explain. Check that your Social Security number, your address(es), name or initials, and your employers are listed correctly. If you find inaccurate or fraudulent information, get it fixed or removed. Visit **www.ftc.gov/idtheft** to learn how.

- **Ask for a copy of your medical records.** If you believe you've already been a victim of medical identity theft, review your medical and health insurance records regularly. The thief may have used your name to see a doctor, get prescription drugs with your health ID number, file claims with your insurance provider, or done other things that leave a trail in your medical records. Try to review your health records for inaccuracies **before** you seek additional medical care. The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule gives you the right to copies of your records that are maintained by health plans and medical providers covered by that law. Health care providers and health plans generally are required to give you your files within 30 days after you ask for them. Unlike credit reports, there is no central source for your medical records. You need to contact each provider you do business with – including doctors, clinics, hospitals, pharmacies, laboratories and health plans – that is relevant to your experience. For example, if a thief got a prescription in your name, you may want the record from the pharmacy that filled the prescription and the health care provider who wrote the prescription. Or if you've been using the same hospital for 20 years and you think that the identity theft is recent, you may want to limit your request to records of the last few years or months.

It's likely that you have to complete a form and pay a fee to get a copy of your records. Keep track of your communications with your health plan and providers, including copies of postal and email correspondence, and a log of your phone calls, conversations and activities. Be patient: Health plans and providers, particularly small ones, may not have handled a claim of medical identity theft before, and may not be sure how to respond.

In most instances, a provider who denies you access to your records must give you the reason in writing. Some providers may refuse to give you copies of your medical or billing records for fear that they're violating the identity thief's HIPAA privacy rights. These providers are mistaken: You have the right to know what's in your file. If your request is denied, you have the right to appeal. Contact the person identified in the provider's Notice of Privacy Practices or the patient representative or ombudsman, explain the situation and request your file. If a provider still refuses to give you

access to your records within 30 days of your written request, file a complaint with the U.S. Department of Health and Human Services' Office for Civil Rights, at **www.hhs.gov/ocr**.

You also should get a copy of the accounting of disclosures for your medical record from your health plan and providers. It will help you follow the trail of your information and identify who has incorrect information about you. The law allows you to order one free copy of the accounting from each of your providers every 12 months. The accounting is a record of:

- the date of the disclosure;
- the name of the person or entity who received the information;
- a brief description of the information disclosed;
- a brief statement of the purpose of the disclosure or a copy of the request for it.

Certain disclosures that occur often or as a matter of routine – like each time a doctor's office sends treatment information to another health care provider, or sends payment information to an insurer for reimbursement – may not be included in the accounting.

For more information about your rights under HIPAA, visit the U.S. Department of Health and Human Services, Office for Civil Rights at **www.hhs.gov/ocr**, or the World Privacy Forum at **www.worldprivacyforum.org/FAQ_medicalrecordprivacy.html**.

Bouncing Back from Medical Identity Theft

If you are a victim of medical identity theft, here are several steps to take immediately. Keep detailed records of your conversations and copies of your correspondence.

1. **File a complaint with the Federal Trade Commission** online at **https://www.ftccomplaintassistant.gov** or by phone at 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261.

2. **File a report with your local police,** and send copies of the report to your health plan's fraud department, your health care provider(s), and the three nationwide credit reporting companies. Information on how to file a police report is at **www.ftc.gov/idtheft/consumers/defend.html**.

3. **Exercise your right under HIPAA to correct errors in your medical and billing records.** Write to your health plan or provider detailing the information that seems inaccurate. Include copies (keep the originals) of any document that supports your position. In addition to providing your complete name and address, your letter should identify each item in your record that you dispute, state the facts and your reasons for disputing the information, and request that each error be corrected or deleted. You may want to enclose a copy of your medical record with the items in question circled. Send your letter by certified mail, and ask for a "return receipt," so you can document what the plan or provider received. Keep copies of your dispute letter and enclosures.

   Generally, your health plan or medical provider must respond: The creator of the information

is obligated to amend the inaccurate or incomplete information. It also should notify other parties, like labs or other health care providers, that may have received incorrect information. If an investigation doesn't resolve your dispute with your plan or provider, you can ask that a statement of the dispute be included in your record.

Other Steps to Consider

A **fraud alert** can help prevent an identity thief from opening additional accounts in your name. Contact the toll-free fraud number of any one of the three nationwide credit reporting companies to place a fraud alert on your credit report. Contact only one of the three companies to place an alert. The one you call is required to contact the others that, in turn, place an alert on their versions of your report, too.

- TransUnion: 1-800-680-7289; **www.transunion.com**; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790
- Equifax: 1-800-525-6285; **www.equifax.com**; P.O. Box 740241, Atlanta, GA 30374-0241
- Experian: 1-888-EXPERIAN (397-3742); **www.experian.com**; P.O. Box 9554, Allen, TX 75013

A **security freeze**, also known as a credit freeze, is a warning sign to businesses or others who may use your credit file. It locks down your credit file and blocks access by potential creditors. In short, it makes it less likely that an identity thief can open new accounts. Most states have laws that allow consumers to place a credit freeze with credit reporting companies. In many of these states, any consumer can freeze their credit file; in others, only identity theft victims can freeze their files.

Placing a credit freeze does not affect your credit score, keep you from getting your free annual credit report, or keep you from buying your credit report or score. It doesn't prevent you from opening a new account, applying for a job, renting an apartment, or buying insurance, either. In these situations, the business usually needs to review your credit report. You can ask the credit reporting company to lift your credit freeze temporarily, or remove it altogether.

There are two key differences between security freezes and fraud alerts:

- The credit reporting companies are not required to share a request for a security freeze as they are with a fraud alert. If you want to freeze all your credit files completely, you have to contact each company with your request.
- The credit reporting companies may charge you a fee to place a freeze or to lift it. The fees and lead times to freeze or "thaw" your credit file vary among states, so it's wise to check with your state authorities or with a credit reporting company in advance if possible. In many states, security freezes are free for identity theft victims; in others, consumers must pay a fee – typically $10. It's also important to know that each credit reporting company charges a fee for this. More information is at **www.ftc.gov/idtheft**.

If you have a valid police or other investigative report about the theft, you usually can place or lift a freeze for free.

If you believe you are a victim of medical identity theft and are concerned that your identity could be compromised further – say, by credit accounts being opened in your name – you may want to consider a freeze as an additional layer of protection.

For More Information

For information about getting and correcting your medical records:

World Privacy Forum
2033 San Elijo Avenue, #402
Cardiff by the Sea, CA 92007
www.worldprivacyforum.org
760-436-2489

Center on Medical Record Rights and Privacy
Health Policy Institute
Georgetown University
Box 57144
Washington, DC 20057-1485
http://ihcrp.georgetown.edu/privacy/records.html
202-687-0880

If you believe that a health plan or provider violated your rights under HIPAA, you may want to file a complaint with:

U.S. Department of Health and Human Services
Office for Civil Rights
200 Independence Avenue, SW
Washington, DC 20201
www.hhs.gov/ocr

The FTC works to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them. To file a complaint or get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. Watch a new video, How to File a Complaint, at ftc.gov/video to learn more.

The FTC enters consumer complaints into the Consumer Sentinel Network, a secure online database and investigative tool used by hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Federal Trade Commission	ftc.gov
1-877-FTC-HELP	For The Consumer

Federal Trade Commission
Bureau of Consumer Protection
Division of Consumer and Business Education

January 2010