

Medical ID Theft



Medical ID theft: Medical ID theft occurs when a thief uses your personal information, such as your name, Social Security number or health insurance ID, to get medical care, submit fake billing claims, buy drugs or purchase expensive medical equipment. According to an article published on NBCNews.com, medical ID theft is one of the most costly, confusing and potentially dangerous types of fraud—and according to a study by the Ponemon Institute, it's on a sharp rise. Ponemon estimates that more than 2.3 million adult Americans or close family members became victims in 2014.

Medical ID theft can have serious consequences. It can disrupt your life, not only in monetary damages, but also in compromised personal medical records that can result in misdiagnosis, mistreatment or incorrect prescriptions. If wrong information ends up in your personal medical records, it can be life threatening. In addition, once someone becomes a victim, it's extremely difficult to untangle the fraudulent bills and ruined medical records.

Ponemon's study found that the average victim didn't find out about the theft until three months after it happened, and 30 percent of victims didn't know when the crime occurred. Since, privacy laws protect the release of health information, fixing the problem is difficult. Victims often have to be a part of the investigation, and it can be tough for victims to prove they're not the ones who actually received treatment.

Signs of medical ID theft: According to the Federal Trade Commission (FTC), you may be a victim of medical ID theft if: (1) You get a bill for medical services you didn't receive; (2) A debt collector contacts you about medical debt you don't owe; (3) You order your credit report and see medical debts you don't owe; (4) You try to make a legitimate insurance claim and your health plan says you have reached your benefits limit; or (5) You are denied insurance because your medical records show a condition you don't have. Medical ID theft is a non-credit identity theft crime. Therefore, credit monitoring services, fraud alerts or credit freezes may not alert you to or stop it.

Detecting medical ID theft: According to the FTC, you should read your medical and insurance statements regularly and completely because they can show warning signs of identity theft. Read the Explanation of Benefits (EOB) statement or Medicare Summary Notice that your health plan sends after treatment. Check the name of the provider, the date of service and the service provided. Check to see if the claims paid match the care you received.

Accessing your medical records: The HIPAA Privacy Rule gives consumers the right to inspect, review and receive a copy of their medical and billing records that are held by health plans and health care providers covered by the Privacy Rule. How can consumers make a request for access to their records? Consumers should start by obtaining a copy of the notice of privacy practices (NPP) that the HIPAA Privacy Rule requires each hospital and insurer to publish. The NPP describes a consumer's rights, including their right to inspect and obtain a copy of their medical records. Consumers can use copies of their medical and billing records to determine the impact of a theft and to identify inaccuracies before seeking additional medical care. There is no central source for medical records, so consumers need to contact each provider they do business with—doctors, clinics, hospitals, pharmacies, laboratories and health plans. Find out if your doctor, hospital, pharmacy, lab or health insurance company offers Blue Button. The Blue Button lets you go online and download your health records so you can:

- Make sure the information in your records, such as your medication list, name of provider, dates of service and service provided, is accurate and complete.
- Share them with your doctor or trusted family members or caregivers.
- Keep track of when your child had his/her last vaccination.
- Have your medical history available in case of emergency, when traveling, seeking a second opinion or switching health insurance companies.
- Plug your health information into apps and tools that help you set and reach personalized health goals.

Medicare beneficiaries can view and download their Medicare claims data in a more timely and user-friendly format than ever before through the Medicare Blue Button (www.medicare.gov/manage-your-health/blue-button/medicare-blue-button.html).

Veterans can use the Blue Button on the My HealthVet website (www.myhealth.va.gov) to download demographic information (age, gender, ethnicity and more), emergency contacts, a list of their prescription medications, clinical notes and wellness reminders.

Get an accounting of disclosures: Ask each of your health plans and medical providers for a copy of the “accounting of disclosures” for your medical records. The accounting is a log of who has received copies of your medical records. According to the FTC, the law allows you to order one free copy of the accounting from each of your medical providers every 12 months. The accounting includes details about: (1) what medical information the provider sent; (2) When it sent the information; (3) Who received the information; and (4) Why the information was sent. The accounting shows who has copies of your mistaken records and whom you need to contact.

Correcting mistakes in your record: If after you access your medical records you find mistakes, the FTC suggests that you write your health plan and medical providers and explain which information is not accurate. Send copies of the documents that support your position. You can include a copy of your medical record and circle the disputed items. Ask the provider to correct and/or delete each mistake. Remember to send your letter by certified mail, and ask for a “return receipt” so that you have proof that the plan or medical provider received it.

File a complaint: Patients have the right to file a complaint if they believe their privacy rights have been violated. For example, it would be a violation if a medical provider refused to provide someone with a copy of his or her own medical record. Patients can file a complaint with the U.S. Department of Health and Human Services’ Office for Civil Rights (www.hhs.gov/ocr).

Protecting your medical identity: Guard your medical insurance card as you do your credit card. Carry it only when you’ll need it. Resist sharing your medical identity in exchange for free gifts or services. Shred any medical documents and prescription bottle labels you no longer need. Contact your insurance company, Medicare or local Medicaid office if your insurance card is missing or stolen.

Resources:

- Medicare Summary Notice (Medicare.gov): www.medicare.gov/forms-help-and-resources/mail-about-medicare/medicare-summary-notice.html
- The HIPAA Privacy Rule: Patients’ Rights (Privacy Rights Clearinghouse): www.privacyrights.org/content/hipaa-privacy-rule-patients-rights
- Prevent Medical Fraud (ProtectMyID): www.protectmyid.com/identity-theft-protection-resources/types-of-fraud/medical-fraud.aspx
- Medical Identity Theft (FTC): www.consumer.ftc.gov/articles/0171-medical-identity-theft
- Consumer Tips: Medical Identity Theft: What to Do if You Are a Victim (or are concerned about it) (World Privacy Forum): www.worldprivacyforum.org/2012/04/consumer-tips-medical-id-theft-what-to-do-if-you-are-a-victim/

Consumer Action empowers low- and moderate-income and limited-English-speaking consumers nationwide to financially prosper through education and advocacy. Visit us online at www.consumer-action.org.