

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? 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 get your mail in the post and see medical collections 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

You can minimize your risk of medical identity theft by taking the following steps:

- **Verify a source before sharing information.**

Don't give out your 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 medical reimbursement.

- **Safeguarding 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 national insurance 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 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. Make sure that 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.
- **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. Section 8 of The Data Protection (Privacy of Personal Information) Act, 2003, (DPA) gives you the right to copies of your records that are maintained by health plans and medical providers, within 40 days of your written request.

If your health care provider is uncooperative, you may lodge a complaint with the Office of the Data Protection Commissioner. Refer to our website www.bahamas.gov.bs/dataprotection for information on how to lodge a complaint.

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 your medical insurance provider under advice to the Data Protection Commissioner, as quickly as possible.
2. File a report with the Police and send copies of the report to your health plan's fraud department and your health care provider.
3. Exercise your right under the DPA to correct errors in your medical and billing records. Write to your health plan 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 item in question circled. Send your letter by registered 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.

For more information on this and any other data protection concern you may have, please email us at dataprotection@bahamas.gov.bs or visit our website www.bahamas.gov.bs/dataprotection.

(Adopted in part from the FTC, USA).