

Program Safeguard Contractor

Are You a Victim of Identity Theft?

A group of unknown individuals are soliciting personal identification information from physicians through various corrupt schemes. Once obtained, the personal information is being used to complete fraudulent Medicare provider applications for new practice locations. Once the new provider number is established, these individuals rapidly submit a large volume of claims to the Medicare Carrier for payment.

You May Be a Victim and Not Know It!

In one instance, a provider received a fax on what appeared to be the Carrier's letterhead. The fax was labeled "CMS File Update" and asked for a series of documents, including copies of the physician's medical license and driver's license. The physician faxed the requested information to a toll-free "877" number. The unknown party then submitted a Medicare provider application (CMS 855) under the provider's name and set up a 'fake' office in another city. The real physician discovered the fraud when a third party insurer contacted him for a refund on a patient that was not his.

In another scenario, advertisements were placed in newspapers seeking resumes and other personal information. Prospective job applicants completed applications and submitted copies of medical and/or driver's licenses. This information was then used to establish new Medicare provider numbers and open bank accounts in the physicians' names without their knowledge.

Protect Your Identity!

If you have recently received a phone call or fax from an alleged Contractor employee asking for a "CMS File Update", please contact the provider enrollment department immediately for verification. If you have responded to an employment opportunity which, in retrospect seems suspicious, again contact the provider enrollment department so the information may be forwarded to the Program Safeguard contractor (PSC). Remember, it takes all of us working together to protect the Medicare Trust Fund.

Common Sense Tips!

1. Perform rigorous research regarding opportunities presented to you when making application for joint venture opportunities of companies unknown to you.
2. Remove any unnecessary personal identifying information from outgoing correspondence.
3. Do not post your resume on line, especially if it contains any confidential personal identifying information.
4. Remember, no one from Medicare will contact you to verify your Medicare numbers. They already have this information.

5. Don't leave laptops or other gateways into your personal information unattended.
6. Cancel computer access immediately when anyone leaves your employment.
7. Perform rigorous research regarding the company you intend to work for when applying for employment prior to sharing any personal information.
8. Check with your Carrier to see what practice locations they have listed for you.
9. Contact the OIG Hotline if you suspect you are the victim of provider identity theft:

Phone:
1-800-HHS-TIPS
(1-800-447-8477)

E-Mail:
HHSTips@oig.hhs.gov

Fax:
1-800-223-8164

Mail:
Office of Inspector General
Department of Health and Human Services
Attn: HOTLINE
PO Box 23489
Washington, DC 20026

TTY:
1-800-377-4950