

FRAUD ALERT



Friday December 16, 2011

Please share this Fraud Alert with colleagues, consumers, or other professionals in your area. If you have any questions about the Illinois SMP program, or to receive these Fraud Alerts directly, please contact Erin Weir, Healthcare Consumer Protection Coordinator at AgeOptions.

Fraud In The News

The following are current news articles about health care and fraud issues.

Health Care Fraud:

1. "New CMS Program to Assist Physician ID Theft Victims"(amednews.com):
<http://www.ama-assn.org/amednews/2011/12/05/gvdsd1205.htm>
2. "KC Woman, St. Louis Man Plead Guilty to Medicaid Kickbacks" (U.S. Department of Justice press release):
<http://www.justice.gov/usao/mow/news2011/broadway.ple.html>

Consumer Fraud:

3. "Counties Warn of Juror ID Theft Scam" (Scam Warning from Kane and McHenry Counties featured in the Daily Herald):
<http://www.dailyherald.co>

Dear SMP readers,

This week's Fraud Alert contains information about new CMS efforts to fight prescription drug fraud, warnings about two email scams, and educational videos and podcasts on health care fraud topics from the U.S. Department of Health and Human Services Office of the Inspector General.

Have a great weekend!

What you will find in this week's Fraud Alert

- CMS Expands Efforts to Fight Fraud in Drug Program
- Open Enrollment Period Email Scam
- Better Business Bureau Warns About Spam Email
- OIG Releases Health Videos and Audio Podcasts on Kickbacks, Care Provider Compliance

CMS Expands Efforts to Fight Fraud in Drug Program

This week, the Obama Administration announced recovery of \$5.6 billion in fraudulent payments in fiscal year 2011, a 167% increase over 2008. They also announced that CMS will be taking additional steps to crack down on fraud and abuse in the Medicare Part D prescription drug program. The full press release that announces the steps being taken is available here:

<http://www.cms.gov/apps/media/press/factsheet.asp?Counter=4217>

Open Enrollment Period Email Scam

The Delaware SMP shared a report this week of an email "phishing" scam. The email subject line reads "Medicare Enrollment Extended: Find a Plan!" Attached to the email is an image that says "Medicare Open Enrollment Ends February 2012. Don't Lose Your Benefits!" The image also contains a link button that says "Find a Plan" and lists several major insurance companies. **This statement is false – the time for Medicare beneficiaries to change their plans was October 15-December 7.**

The email came from a strange looking email address; we suspect that it is an attempt to get people to follow a link and give personal information to a scam artist. It is important to never click on links or open attachments in emails that come from unknown sources, regardless of how 'professional' the email may look – they are generally scams, and

[m/article/20111212/news/712129756/](http://www.ftc.gov/opa/2011/11/11/privacysettlement.shtml)

4. “Facebook Settles FTC Charges That It Deceived Consumers By Failing to Keep Privacy Promises” (FTC announcement):
<http://www.ftc.gov/opa/2011/11/11/privacysettlement.shtml>
5. “AARP Scam Alert: Spammers Get Up Close and Personal”:
<http://www.aarp.org/money/scams-fraud/info-12-2011/spammers-target-email-accounts-scam-alert.html?cmp=NLC-RSS-DAILY-BULLETIN>

they may contain viruses or other malware. Also, never give personal information away in response to an email, or through a link you receive in an email. If you receive an email that you think may be from a legitimate source, such as your bank, contact that source by phone first and give them your information that way.

Better Business Bureau Warns About Spam Email

The Texas SMP program shared a warning last week about a spam email claiming to come from the Council of Better Business Bureaus. The subject line says “Complaint from your customers.” The email includes the Council of Better Business Bureau’s address to make it seem more legitimate, but the email includes a malicious link to a non-BBB website.

As mentioned above, never click on any links in emails from unknown sources, even when they claim to be from a legitimate business or government entity. If you want to know if an email is real, contact the legitimate source by phone to verify before sharing any information, and only visit websites by typing the legitimate address into a web browser yourself – **not** by clicking on links received via email.

OIG Releases Videos and Audio Podcasts on Kickbacks, Health Care Provider Compliance

The U.S. Department of Health and Human Services Office of the Inspector General (OIG) has released videos and podcasts on a number of health care fraud related topics. In the last couple of weeks, they have posted videos and podcasts explaining kickbacks and the laws prohibiting them, as well as compliance training videos for health care providers. These educational videos and podcasts on a variety of topics will continue to be released once a week for the next three months. All of the videos and podcasts are available here:

<http://oig.hhs.gov/newsroom/podcasts/>



Erin Weir, MSW, LSW, Healthcare Consumer Protection Coordinator

AgeOptions

1048 Lake Street, Suite 300

Oak Park, IL 60301

phone (708)383-0258 fax (708)524-0870

erin.weir@ageoptions.org

ageoptions.org

AgeOptions, the Area Agency on Aging of Suburban Cook County, is committed to improving the quality of life and maintaining the dignity of older adults and those who care about them – through leadership and support, community partnerships, comprehensive services, accurate information and powerful advocacy.

Fraud Alerts contain information about current scams taking place in Illinois, announcements and updates about programs or services related to health care and/or fraud protection, and links to news articles about health care and fraud topics. Please forward any recommendations or announcements that you would like to be included in a future Fraud Alert to erin.weir@ageoptions.org.