DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850


**Center for Program Integrity**

Date: November 13, 2013

To: All Medicare Advantage Organizations (MAOs) and Prescription Drug Plan Sponsors (PDPs)

From: Mark Majestic, Acting Director
Medicare Program Integrity Group (MPIG)

Re: Identify Theft

The Centers for Medicare & Medicaid Services (CMS) has been made aware of information involving individuals who are engaged in a scheme to obtain employment with Medicare Advantage and Prescription Drug Plan Sponsors in order to steal the identities of members in furtherance of a credit card and/or tax refund fraud scheme.

According to information received from a plan sponsor, an employee, hired through a temporary agency, was making screen printouts of member information that were then used to file credit card applications and false 2012 tax returns; both listed addresses other than the member's residence. Most of the elderly members were no longer filing tax returns for the 2013 Tax Season and were unaware of the fraud. The employee also conducted Internet research during work hours to obtain the names of deceased individuals that were used to file false tax returns.

The plan's investigation determined that the temporary agency that supplied the employee did not conduct an adequate background check that would have identified the individual's criminal history.

**Requested Action**

The following are recommendations for plan sponsors to consider mitigating security breaches by employees and theft of members' identities:

1. Conduct comprehensive background investigations of all employees
    a) All Medicare Advantage Plans and Prescription Drug Plan Sponsors must adhere to Compliance Program Guidelines which require plan sponsors to review the DHHS OIG List of Excluded Individuals and Entities (LEIE) and the GSA System of Award Management (SAM) prior to the hiring or contracting of any new employee, temporary employee, volunteer, consultant, governing body

member, or FDR are excluded or become excluded from participation in federal programs.

b) Consider contracting directly with entities that conduct comprehensive background checks for all existing and potential employees.

i. Do not rely on background checks conducted by temporary employment agencies.
ii. Checks should include criminal and financial history of the prospective employee.
iii. Consider not permitting temporary employees to have access to PII, PHI, or to financially sensitive information

2. Perform Proper Oversight of employees' work products

a) Obtain software that is able to identify any of the following issue with employees improperly accessing potentially sensitive records: Software should alert a supervisor to outliers such as pages/print screen containing personally identifiable information (PII) and protected health information (PHI) information, which is outside the normal course of conducting business.

b) Software should create an audit trail of which files, cases, or members an employee views. The audit trail should track the date and time the information was viewed.

c) The information should to be placed in a virtual "format" to observe an employee's work in real time.

3. Implement safeguards to limit:

a) Access to PHI/PII to those employees that require the information to perform their job.

4. Monitor and audit internet searches:

a) Limit access to social media and research sites that are not needed to perform the employees' assigned task.
b) Note unusual searches that are not associated with job responsibilities and could potentially pose harm/threat (e.g., Ancestry.com, Google.com)

5. Secure containers to deposit confidential documents (containing PII/PHI) for shredding. Use employees to monitor collection of materials to be shredded.

6. Frequent internal training of staff regarding protection of PHI and PII and the consequences of compromising the identities of members.

7. Scrutinize data to detect unusual patterns that my signify billing for services not rendered.

If you identify compromised beneficiaries or have information related to this scheme, take the appropriate actions to protect Medicare beneficiaries and contact Health Integrity, the National Benefit Integrity Medicare Drug Integrity Contractor (NBI MEDIC), at 1-877-7SAFERX. Any questions on this subject should be directed to Benefit Integrity Manager Martina Gilly of the NBI MEDIC at gillym@healthintegrity.org or your CMS Account Manager.