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

CENTERS for MEDICARE & MEDICAID SERVICES

CENTER FOR DRUG AND HEALTH PLAN CHOICE

MEMORANDUM

Date: December 16, 2008

To: Medicare Advantage Organizations
Medicare Advantage – Prescription Drug Organizations
Cost-Based Contractors
Prescription Drug Plan Sponsors
Employer/Union Sponsored Group Health Plans

From: Abby L. Block **/s/**
Director, Center for Drug and Health Plan Choice

Subject: Security and Privacy Reminders and Clarification of Reporting Procedures

Ensuring Security and Protection of Personally Identifiable Health Information (PII)

On June 9, 2006, the Centers for Medicare & Medicaid Services (CMS) sent a Health Plan Management System (HPMS) memorandum to all Medicare Advantage Organizations and Prescription Drug Plans, reminding them of the necessity of effectively securing all beneficiary information, whether in paper or electronic format. As we are in the Annual Enrollment Period, we wish to remind plans of the need to protect sensitive beneficiary data.

As described in this memorandum and other CMS guidance, some measures organizations should take to protect the security and privacy of personally identifiable information (PII) include:

- Ensuring that data files are not saved on public or private computers when accessing corporate e-mail through the Internet.
- Ensuring that electronic systems are properly programmed for beneficiary mailings in order to prevent documents containing PII from being sent to the wrong beneficiaries.
- PII data on all portable devices are encrypted (as referenced in the 2009 Call Letter).
- Implement security measures to restrict access to PII based on an individual's need to access the data.
- Perform an internal risk assessment or engage an industry-recognized security expert to conduct an external risk assessment of the organization to identify and address security vulnerabilities.
- Quickly remedy weaknesses or gaps in your security program.

- Train staff on responsibilities and consequences of failing to secure sensitive beneficiary information.
- Document compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security and Privacy rules and keep current in response to environmental or operational changes affecting the security of the electronic protected health information.

As a measure to prevent security breaches, plans should also ensure that all down-stream entities are aware of their responsibility to protect PII data and report suspected breaches. You should remind agents and brokers of their responsibility to protect beneficiary information. Plans using offshore subcontractors must ensure their compliance with the requirements contained in the July 23, 2007, HPMS memorandum.

If there are any security incidents, including those of a down-stream entity, it is the responsibility of the plan to report this information to CMS, per the instructions below.

Reporting Incidents to CMS

A security incident is the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system. It also includes the potential loss of PII through theft or device misplacement, loss or misplacement of hardcopy documents, and misrouting of mail.

CMS is releasing this guidance to provide clear instructions on the manner and timeframe in which organizations should report security incidents, including those involving personally identifiable information (PII). Plans should immediately notify CMS of any incident involving a security incident using the following steps:

- Review business partner arrangements and ensure that all business associate agreements are current in order to prevent unauthorized access to data.
- Contact the CMS Information Technology (IT) Service Desk at 1-800-562-1963 to report the security incident and obtain a ticket number. Record your ticket number. The CMS IT Service Desk is the first point of contact for reported operational problems and security incidents.
- Notify your CMS Account Manager of the incident and provide them with your CMS IT Service Desk ticket number.
- Submit the reported incident to the CMS IT Service Desk at: cms_it_service_desk@cms.hhs.gov with a copy to your CMS Account Manager. You should include your parent organization name in the subject line along with the ticket number.
    - If the security incident does *not* involve PII, your organization should complete the information contained in the form in Exhibit A.
    - If the security incident involves PII, your organization should complete the information contained in the form in Exhibits A and Exhibit B.

- This information must be reported in a timely manner. The information incident categories and reporting time criteria are set forth in Exhibit C.
- Your CMS Account Manager will be your point of contact in communicating next steps, including:
  - Whether additional reporting is required (e.g., to provide corrective action steps taken in response to the incident);
  - Whether beneficiary or provider notification is required;
  - The appropriate type of communication (e.g., press release, letters, etc.); and
  - Whether credit protection services should be provided.

For questions regarding this memorandum, please contact Brandon Bush at (410) 786-0228. Thank you for your continued support of the protection of Medicare beneficiaries' PII.