CMS Manual System	**Department of Health & Human Services (DHHS)**
Pub 100-08 Medicare Program Integrity	**Centers for Medicare & Medicaid Services (CMS)**
Transmittal 211	**Date: JUNE 22, 2007**
	Change Request 5581

SUBJECT: Medicare Benefit Vulnerability Reporting

I. SUMMARY OF CHANGES: In accordance with the Improper Payments Information Act (IPIA) of 2002, the Centers for Medicare and Medicaid Services (CMS) is required to review all its programs annually to identify areas of risk that could result in improper payments, and to take corrective actions to mitigate those risks. CMS serves as a focal point for IPIA related activities, specifically CERT and PERM Error Rate Measurement Programs. We play a major role for identifying potential vulnerabilities to the Medicare program through data analysis/mining. Vulnerabilities are defined as an instance of potential Medicare fraud, waste, or abuse identified though the analysis and management of provider, supplier, and beneficiary data.

Our goals is to develop a central repository for all Medicare program vulnerability data. Centralized data gathering will allow for the identification of new vulnerabilities and reduced duplication.

NEW / REVISED MATERIAL
EFFECTIVE DATE: APRIL 2, 2007
IMPLEMENTATION DATE: JULY 23, 2007

Disclaimer for manual changes only: The revision date and transmittal number apply only to red italicized material. Any other material was previously published and remains unchanged. However, if this revision contains a table of contents, you will receive the new/revised information only, and not the entire table of contents.

II. CHANGES IN MANUAL INSTRUCTIONS: (N/A if manual is not updated)
R=REVISED, N=NEW, D=DELETED

R/N/D	CHAPTER / SECTION / SUBSECTION / TITLE
R	4/4.31/Vulnerability Report

III. FUNDING:

No additional funding will be provided by CMS; contractor activities are to be carried out within their FY 2007 operating budgets.

IV. ATTACHMENTS:

Business Requirements
Manual Instruction

Unless otherwise specified, the effective date is the date of service.

Attachment - Business Requirements

Pub. 100-08	Transmittal: 211	Date: June 22, 2007	Change Request: 5581

SUBJECT: Medicare Benefit Vulnerability Reporting

EFFECTIVE DATE: April 2, 2007

IMPLEMENTATION DATE: July 23, 2007

I. GENERAL INFORMATION

A. Background: In accordance with the Improper Payments Information Act (IPIA) of 2002, the Centers for Medicare & Medicaid Services (CMS) is required to review all its programs annually to identify areas of risk that could result in improper payments, and to take corrective actions to mitigate those risks. CMS serves as a focal point for IPIA related activities through the CERT and PERM Error Rate Measurement Programs and identifies potential vulnerabilities to the Medicare program through data analysis / mining. Vulnerabilities are defined as an instance of potential Medicare fraud, waste, or abuse identified though the analysis and management of provider, supplier, and beneficiary data.

Centralized Medicare program vulnerability data gathering will allow for the identification of the top ten overall Medicare program vulnerabilities. Further, centralized data gathering will allow for easier tracking of vulnerabilities for resolution on a national / regional level, and quick sharing of risks and corrective actions with CMS partners through avenues such as the Vulnerability Report shown at the end of section 4.31.

B. Policy: N/A

II. BUSINESS REQUIREMENTS

"Shall" denotes a mandatory requirement

Requirement Number	Requirements	Responsibility ("X" indicates the columns that apply)							
		FI	DMERC	PSC	RHHI	*Carrier*	A/B MAC	DME MAC	QIO

5581.1	The PSC BI units shall submit any identified program vulnerabilities in the appropriate narrative in the PSC monthly cost report. The PSC BI units shall also send identified vulnerabilities to the vulnerability mailbox.			X					
5581.2	FIs, PSCs, RHHIs, carriers, A/B MACs, DME regional carriers, and DME MACs shall submit any identified program vulnerabilities to the vulnerability mailbox regardless of risk level, as soon as possible after they are discovered, however no less than on a quarterly basis. Reports should be submitted no later than fourteen business days after the end of each calendar quarter.	X	X	X	X	X	X	X	X
5881.3	The identified vulnerability reports shall include how the vulnerability was discovered, a summary of the issues, a description of the methodology, recommendations for resolving the vulnerability, and any action taken to resolve the vulnerability.	X	X	X	X	X	X	X	X
5581.4	FIs, PSCs, RHHIs, carriers, A/B MACs, DME regional carriers, and DME MACs shall send the reports to the vulnerability mailbox at the following address: vulnerability@cms.hhs.gov.	X	X	X	X	X	X	X	X

III. PROVIDER EDUCATION TABLE

Number	Requirements	Responsibility ("X" indicates the columns that apply)						
		FI	PSC	RHHI	Carrier	A/B MAC	DME MAC	QIO
	None							

IV. SUPPORTING INFORMATION

A. Recommendations and Supporting Information Associated with Listed Requirements: N/A

X-Ref Requirement #	Recommendation or other supporting information:

B. All Other Recommendations and Supporting Information: N/A

V. CONTACTS

Pre-Implementation Contact(s): Jennifer Smith, jennifer.smith@cms.hhs.gov
Post-Implementation Contact(s): Lameka Davison, lameka.davison@cms.hhs.gov

VI. FUNDING

A. For FIs, PSCs, RHHIs, QIOs, and Carriers:

No additional funding will be provided by CMS; contractor activities are to be carried out within their FY 07 operating budget.

B. For A/B MACs and DME MACs:

The contractor is hereby advised that this constitutes technical direction as defined in your contract. CMS does not construe this as a change to the Statement of Work (SOW). The contractor is not obligated to incur costs in excess of the amounts allotted in your contract for your FY 2007 operating budget unless and until specifically authorized by the contracting officer. If the contractor considers anything provided, as described above, to be outside the current scope of work, the contractor shall withhold performance on the part(s) in question and immediately notify the contracting officer, in writing or by e-mail, and request final directions regarding continued performance requirements.

4.31 – Vulnerability Report

(Rev.211, Issued: 06-22-07, Effective: 04-02-07, Implementation: 07-23-07)

Program vulnerabilities can be identified through a variety of sources such as the Chief Financial Officer's (CFO) Audit, Fraud Alerts, the General Accounting Office (GAO), the Office of Inspector General (OIG), data driven studies, and PSC and Medicare contractor operations, as examples. The PSC BI units shall submit any identified program vulnerabilities in the appropriate narrative in the PSC monthly cost report. The PSC BI units shall also send identified vulnerabilities to the vulnerability mailbox. FIs, PSCs, RHHIs, carriers, QIOs, A/B MACs, and DME MACs shall submit any identified program vulnerabilities to the vulnerability mailbox regardless of risk level, as soon as possible after they are discovered, however no less than on a quarterly basis. Reports should be submitted no later than fourteen business days after the end of each calendar quarter, but can be submitted sooner if the vulnerability requires immediate consideration. Contractors are not prohibited from initiating any actions in regards to fraud, waste, or abuse situations regardless of whether the vulnerability has been reported yet. The identified vulnerability reports shall include how the vulnerability was discovered, a summary of the issues, a description of the methodology, recommendations for resolving the vulnerability, and any action taken to resolve the vulnerability.

The FIs, PSCs, RHHIs, carriers, QIOs, A/B MACs, and DME MACs shall send the quarterly reports to the vulnerability mailbox at the following address: **vulnerability@cms.hhs.gov**.

Vulnerability Report VR-1-022007

Topic:

Submitted by: Name Organization:
Phone: E-mail:

Source:
Current Contact:

SUMMARY OF POTENTIAL VULNERABILITY

FINDINGS

SUMMARY SUPPORTING DATA

.

ACTIONS TAKEN OR RECOMMENDED

RELATED VRs