Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

ADDRESSING VULNERABILITIES REPORTED BY MEDICARE BENEFIT INTEGRITY CONTRACTORS

Daniel R. Levinson
Inspector General

December 2011
OEI-03-10-00500

OBJECTIVES

1. To determine the extent to which the Centers for Medicare & Medicaid Services (CMS) has resolved vulnerabilities reported by Medicare benefit integrity contractors.
2. To determine the monetary impact of the reported vulnerabilities on the Medicare program.
3. To review CMS's procedures for tracking, reviewing, and resolving reported vulnerabilities.

BACKGROUND

One way that Medicare benefit integrity contractors help prevent fraud, waste, and abuse is by identifying program vulnerabilities. This report provides information on the vulnerabilities reported by Medicare benefit integrity contractors in 2009. Within Medicare Parts A and B, Program Safeguard Contractors (PSC) and Zone Program Integrity Contractors (ZPIC) are responsible for benefit integrity; within Parts C and D, Medicare Drug Integrity Contractors (MEDIC) perform that function. PSCs, ZPICs, and MEDICs are required to submit periodic vulnerability reports to CMS. These reports describe vulnerabilities and may include recommendations for resolving them. These reports also may contain the monetary impact of the vulnerabilities on Medicare. For this study, we determined the number and monetary impact of vulnerabilities reported by PSCs, ZPICs, and MEDICs in 2009. We reviewed the actions that CMS took to address or resolve these reported vulnerabilities. We also reviewed CMS's policies and procedures for tracking, reviewing, and resolving the reported vulnerabilities.

FINDINGS

As of January 2011, CMS had not resolved or taken significant action to resolve 77 percent of vulnerabilities reported by contractors in 2009. Of the 62 vulnerabilities reported by contractors in 2009, 48 (77 percent) had not been resolved as of January 2011, nor had CMS taken significant action to resolve them. CMS indicated that of these 48 reported vulnerabilities, 20 were "currently under review" and 3 required additional analysis to determine whether they were actual vulnerabilities. For the remaining 25, we determined from CMS's description that no action was taken or that the action taken was not significant. CMS took significant action to resolve 14 of the 62 reported

vulnerabilities, but only 2 of these 14 had been fully resolved by January 2011.

Over half of the vulnerabilities submitted by contractors included detailed recommendations for CMS to resolve the vulnerabilities; however, most of the actions that CMS reported taking to resolve them were not the result of these contractor recommendations.

Coding and/or billing vulnerabilities were the most common type of vulnerability reported by PSCs and ZPICs. Vulnerabilities related to provider identifiers were the most common type of vulnerability reported by MEDICS.

Contractors reported monetary impact for only one-third of vulnerabilities, but their estimated impact was $1.2 billion. Only 21 of the 62 vulnerabilities had an associated monetary impact reported by the contractor. According to CMS staff, PSCs and ZPICs are required to report monetary impact, but less than half of their reports included this information. MEDICs are not required to report monetary impact.

The estimated impact of these 21 vulnerabilities was $1.2 billion, with the estimated impacts of individual vulnerabilities ranging from $77,692 to $803,025,113. None of these vulnerabilities had been resolved as of January 2011, although CMS had taken significant action to resolve four of them, including the two with the largest monetary impact ($803 million and $99 million). For these two vulnerabilities, implementation of corrective actions will not be complete until 2012.

The monetary impact for the 17 vulnerabilities that were not resolved or for which significant action had not been taken was estimated to be $202 million.

Because monetary impact was reported inconsistently or not at all, the actual monetary impact of the vulnerabilities reported in 2009 could be significantly greater than $1.2 billion.

Although CMS has recently begun developing procedures to consistently track and review vulnerabilities, it lacks procedures to ensure that they are resolved. The CMS divisions responsible for tracking and reviewing vulnerabilities have procedures that outline the general steps that they take to perform these tasks. Although contractors have been submitting vulnerability reports for several years, CMS did not begin developing these procedures until June 2010. Furthermore, only one of these CMS divisions has developed procedures to follow up on the implementation of corrective actions to resolve vulnerabilities.

RECOMMENDATIONS

One of the ways that Medicare benefit integrity contractors help prevent fraud, waste, and abuse is by identifying program vulnerabilities. To minimize the financial impact on Medicare, CMS needs to take prompt action to resolve vulnerabilities. Only two of the vulnerabilities reported in 2009 had been resolved as of January 2011.

Most of the vulnerability reports from 2009 did not contain information on monetary impact, and in those that did, monetary impact was not reported consistently. Furthermore, none of the vulnerabilities with reported monetary impact had been resolved. Significant action had been taken to resolve two of the vulnerabilities with the greatest monetary impact ($803 million and $99 million). However, implementation of these actions will not be complete until 2012, 3 years after the vulnerabilities were reported.

For CMS to gain sufficient oversight of program vulnerabilities, it must have policies and procedures for ensuring the prompt resolution of vulnerabilities. In 2011, CMS was still reviewing vulnerabilities reported in 2008 and 2009 to determine whether they had been resolved or whether action still needed to be taken to resolve them.

Therefore, we recommend that CMS:

Determine the status of all vulnerabilities that have not been resolved and take action to address them

Require all benefit integrity contractors to report monetary impact, when calculable, in a consistent format

Ensure that vulnerabilities are resolved by establishing formal written procedures that include timeframes for followup and that outline CMS and contractor responsibilities regarding vulnerability resolution

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

CMS concurred with our first recommendation and is determining the status of all open vulnerabilities and taking action, when possible, to address them. CMS stated that it has determined the status of all MEDIC-identified vulnerabilities.

CMS did not concur with our second recommendation. CMS stated that it would be challenging to require all benefit integrity contractors to report the monetary impact for each vulnerability and to use it in a

consistent methodology. CMS noted that it could be labor intensive for the contractors to determine the dollars at risk for vulnerabilities and that not all vulnerabilities have a monetary impact that results in a loss to the Medicare Trust Fund. Furthermore, CMS stated that different types of vulnerabilities would require different methods of calculating or estimating the monetary impact or would even make such a determination impossible or very difficult because of the time and resources required. We understand that calculating the monetary impact for some vulnerabilities may not be possible and that different types of vulnerabilities would require different methods of calculating monetary impact. However, for cases in which calculating the monetary impact is too burdensome or time consuming, the contractor should report the vulnerabilities and explain why the monetary impact could not be calculated. Based on CMS's comments, we clarified the wording of this recommendation.

CMS concurred in part with our third recommendation. CMS stated that it has standard operating procedures in place and continues to actively manage reported vulnerabilities on a monthly basis. CMS stated that it can establish timeframes for resolution on a case-by-case basis, but said that it will be difficult to establish standard timeframes because actions and resolutions to address vulnerabilities will vary. Although we agree that actions and resolutions will vary depending on the type of vulnerability, it is possible to have standard timeframes for following up to determine the status of the vulnerabilities.

TABLE OF CONTENTS

INTRODUCTION

OBJECTIVES

1. To determine the extent to which the Centers for Medicare & Medicaid Services (CMS) has resolved vulnerabilities reported by Medicare benefit integrity contractors.
2. To determine the monetary impact of the reported vulnerabilities on the Medicare program.
3. To review CMS's procedures for tracking, reviewing, and resolving reported vulnerabilities.

BACKGROUND

One way that Medicare benefit integrity contractors help prevent fraud, waste, and abuse is by identifying program vulnerabilities. This report provides information on the vulnerabilities reported by Medicare benefit integrity contractors in 2009. Within Medicare Parts A and B, Program Safeguard Contractors (PSC) and Zone Program Integrity Contractors (ZPIC) are responsible for benefit integrity; within Parts C and D, Medicare Drug Integrity Contractors (MEDIC) perform that function. PSCs, ZPICs, and MEDICs are required to submit periodic vulnerability reports to CMS. These reports describe vulnerabilities and may include recommendations for resolving them. These reports also may contain the vulnerabilities' monetary impact on Medicare—information that allows CMS to understand the scope of the vulnerabilities and to prioritize those needing corrective actions. For this study, we determined the number and monetary impact of vulnerabilities reported by PSCs, ZPICs, and MEDICs in 2009. We reviewed the actions that CMS took to address or resolve these reported vulnerabilities. We also reviewed CMS's policies and procedures for tracking, reviewing, and resolving the reported vulnerabilities.

Medicare Integrity Program Contractors

The Health Insurance Portability and Accountability Act of 1996 established the Medicare Integrity Program and required CMS to use contractors to perform specific program integrity activities.[1] These activities include, but are not limited to, cost-report auditing, medical review, provider education, and benefit integrity. CMS awards task orders to these contractors to perform specific duties related to program

[1] P.L. 104-191 § 202, Social Security Act, § 1893(a), 42 U.S.C. § 1395ddd.

integrity. These task orders require contractors to review Medicare data to identify cases of potential fraud, investigate these cases, and refer them to law enforcement.

Program Safeguard Contractors and Zone Program Integrity Contractors. Beginning in 1999, CMS awarded benefit integrity task orders to PSCs to detect and deter fraud and abuse in Medicare Part A and/or Part B. In 2009—the period of review for this study—7 PSCs performed work under 18 benefit integrity task orders, with each task order covering a specific geographic jurisdiction.

CMS is transitioning the work of PSCs to ZPICs. The transition is part of CMS's effort to consolidate fraud-fighting work in Parts A, B, C, and D under one type of contractor, the ZPIC. Seven ZPICs will operate in the following geographic zones:

- Zone 1: American Samoa, California, Guam, Hawaii, the Mariana Islands, and Nevada.
- Zone 2: Alaska, Arizona, Idaho, Iowa, Kansas, Missouri, Montana, Nebraska, North Dakota, Oregon, South Dakota, Utah, Washington, and Wyoming.
- Zone 3: Illinois, Indiana, Kentucky, Michigan, Minnesota, Ohio, and Wisconsin.
- Zone 4: Colorado, New Mexico, Oklahoma, and Texas.
- Zone 5: Alabama, Arkansas, Georgia, Louisiana, Mississippi, North Carolina, South Carolina, Tennessee, Virginia, and West Virginia.
- Zone 6: Connecticut; Delaware; Maine; Maryland; Massachusetts; New Hampshire; New Jersey; New York; Pennsylvania; Rhode Island; Vermont; and Washington, D.C.
- Zone 7: Florida, Puerto Rico, and the U.S. Virgin Islands.

Contracts for six of the seven ZPIC zones were awarded between September 2008 and April 2011. ZPICs became operational in five zones—1, 2, 4, 5, and 7—between February 2009 and February 2011; ZPIC operations in Zone 3 have been delayed because of a postaward protest. The contract for Zone 6 was awarded in September 2011.

ZPICs currently perform work under a benefit integrity task order that includes work for Parts A and B, durable medical equipment, and home health and hospice.

The activities that PSCs and ZPICs perform are established through each type of contractor's Statement of Work (SOW). According to the SOWs for both contractor types, PSCs and ZPICs shall review and analyze a variety of data to focus program integrity efforts by (1) identifying program vulnerabilities; (2) identifying providers for review and investigation within their respective jurisdictions; (3) referring potential fraud, waste, and abuse cases to law enforcement; and (4) pursuing administrative actions.[2]

Medicare Drug Integrity Contractors. The Balanced Budget Act of 1997 established Medicare Part C to allow eligible individuals to enroll in health plans offered by private companies approved by Medicare.[3] The Medicare Prescription Drug, Improvement, and Modernization Act of 2003 established Medicare Part D to provide prescription drug benefits under Medicare beginning January 1, 2006.[4] In September 2006, CMS awarded contracts to three regional MEDICs—West, North, and Southeast—to address potential fraud, waste, and abuse related to Part D benefits. In 2008, CMS added Part C to MEDICs' oversight.

MEDIC West's contract was not renewed when it ended in September 2008. In the 2 months following, CMS transitioned MEDIC West's jurisdiction to the two remaining MEDICs. In fall 2009, CMS again restructured the MEDICs, moving from a regionally based program to two national MEDICs with specific areas of focus. MEDIC Southeast became the national Benefit Integrity (BI) MEDIC, and MEDIC North became the national Compliance and Enforcement MEDIC. The BI MEDIC has responsibility for detecting and deterring fraud, waste, and abuse in Parts C and D nationwide.

Reporting of Vulnerabilities

CMS defines vulnerabilities to the Medicare program as instances of potential fraud, waste, or abuse identified through analyzing and

---

[2] CMS, *Zone Program Integrity Contractor Statement of Work*, § 1.3, p. 49; CMS, *Program Safeguard Contractor Statement of Work*, ch. 7, § 1, p. 58.

[3] The Balanced Budget Act of 1997, P.L. 105-33, Title IV, § 4001; Social Security Act, §§ 1851-1859.

[4] The Medicare Prescription Drug, Improvement, and Modernization Act of 2003, P.L. 108-173, Title I, § 101(a)(2); Social Security Act, § 1860D-1(a)(2), 42 U.S.C. § 1395w-101.

managing data on Medicare providers, suppliers, and beneficiaries.[5] Vulnerabilities may be specific (e.g., providers are receiving multiple payments as a result of incorrect coding) or general and programwide (e.g., vulnerabilities exist in the Part D online application process). The types of vulnerabilities and the ways in which they are addressed may differ depending on the Medicare program involved. The vulnerabilities involving fee-for-service payments in Parts A and B may require an approach different from that used for vulnerabilities involving health plans offered by private companies under Medicare Parts C and D. Some methods through which program vulnerabilities may be resolved are claims processing edits, provider education, or issuance of new regulations.

PSCs and ZPICs are required to submit to CMS monthly narratives of all vulnerabilities identified in the previous month. PSCs and ZPICs use the CMS Analysis, Reporting, and Tracking System (CMS ARTS) to submit these narratives.

Since 2008, PSCs and ZPICs also have been required to submit reports on all vulnerabilities to an electronic vulnerability mailbox, no less than quarterly.[6] According to CMS staff, the vulnerability reports submitted to this mailbox are more descriptive than the narratives submitted to CMS ARTS. Within each vulnerability report, PSCs and ZPICs should include a description of how the vulnerability was discovered, a summary of the issues, a description of the methodology, recommendations for resolving the vulnerability, and any action they took to resolve the vulnerability.[7] CMS staff stated that PSCs and ZPICs are also required to include monetary impact in these reports.

MEDICs are required to submit quarterly vulnerability reports to CMS, listing vulnerabilities they identified during that quarter.[8] The reports should address, to the extent possible, the scope of the vulnerabilities and the extent to which they jeopardize Parts C and D. The MEDICs may also propose to CMS the most effective and efficient ways to address the vulnerabilities. CMS staff stated that MEDICs are not required to include monetary impact in these reports.

---

[5] CMS Manual System, Pub. 100-08, Medicare Program Integrity, Transmittal 211, Change Request 5581, June 22, 2007.

[6] CMS, *Medicare Program Integrity Manual*, Pub. 100-04, ch. 4 § 4.31.

[7] Ibid.

[8] CMS, *Medicare Prescription Drug Integrity Contractor (MEDIC) Statement of Work*, § 8.2.12.

CMS Divisions Responsible for Tracking and Reviewing Vulnerabilities

Two CMS divisions review PSC- and ZPIC-reported vulnerabilities: the Division of Medicare Integrity Contractor Operations (DMICO) within the Center for Program Integrity (CPI) and the Division of Data Analysis (DDA) within the Office of Financial Management.

DMICO takes the lead role in tracking and reviewing PSC- and ZPIC-reported vulnerabilities. It also decides how to address them and how to coordinate with other CMS components in doing so.

DDA identifies and addresses improper payments at a programwide level. To minimize the risk for improper payments, DDA reviews PSC- and ZPIC-reported vulnerabilities to compare them with vulnerabilities reported by Medicare administrative contractors (MAC)[9] and recovery audit contractors (RAC).[10]

The Division of Plan Oversight and Accountability within CPI is responsible for tracking, reviewing, and coordinating efforts to resolve MEDIC-reported vulnerabilities.

Related Studies by the Government Accountability Office

In March 2010, the Government Accountability Office (GAO) issued a report that found that CMS did not establish an adequate process to address vulnerabilities identified by Medicare RACs, which are responsible for postpayment claims review in Medicare Parts A and B.[11] Specifically, GAO stated that CMS "did not develop a plan to take corrective action or implement sufficient monitoring, oversight, and control activities to ensure these significant vulnerabilities were addressed."

In March 2011 testimony before the Senate Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, GAO officials recommended that CMS implement prior report recommendations, including developing a robust

---

[9] MACs process and pay claims for Parts A and B.

[10] RACs conduct postpayment claims reviews to detect and correct past improper payments in Medicare Parts A and B. Unlike PSCs and ZPICs, RACs are not responsible for detecting fraud, waste, and abuse.

[11] GAO, *Medicare Recovery Audit Contracting: Weaknesses Remain in Addressing Vulnerabilities to Improper Payments, Although Improvements Made to Contractor Oversight* (GAO-10-143), March 2010.

process for addressing identified vulnerabilities.[12]

METHODOLOGY

Scope

Our study focused on the vulnerabilities reported by the PSCs, ZPICs, and MEDICs that had benefit integrity task orders in 2009. We chose 2009 because it was the first year in which all three types of contractors were operational. This timeframe also gave CMS time to take action, as we began collecting data in December 2010.

The Zone 4 and Zone 7 ZPICs were not fully operational until February 1, 2009; therefore, the earliest vulnerability reports collected for these 2 ZPICs were from March 1, 2009. The Zone 4 and Zone 7 ZPICs were the only ZPICs that had completed their first contract year in 2009.[13] Additionally, because MEDIC West's contract was not renewed when it ended in September 2008, we did not review vulnerabilities reported by this MEDIC.

Data Collection

In December 2010, we requested from CMS all vulnerability reports submitted by PSCs and ZPICs in 2009. Specifically, we requested the vulnerability narratives submitted by PSCs for 2009 and by ZPICs from February 1, 2009, through December 31, 2009. We also requested the quarterly reports submitted by the MEDICs for 2009.

In January 2011, we received from CMS all vulnerability reports submitted by contractors. These included either the narratives from CMS ARTS or the more detailed vulnerability reports that were submitted to the electronic vulnerability mailbox.

We also asked CMS to provide the following additional information for each vulnerability reported:

- the specific contractor that reported the vulnerability;

[12] *Medicare and Medicaid Fraud, Waste, and Abuse: Effective Implementation of Recent Laws and Agency Actions Could Help Reduce Improper Payments*, Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, Committee on Homeland Security and Governmental Affairs, U.S. Senate, 112 Cong. (March 9, 2011) (Statement of Kathleen M. King, Director of Health Care, and Kay L. Daly, Director of Financial Management and Assurance, GAO).

[13] The first contract year for the Zone 4 and Zone 7 ZPICs was September 30, 2008, through October 31, 2009.

- the date of the report in which the vulnerability was identified;
- a description of the vulnerability;
- a detailed description of any action taken by CMS that resolved or addressed the vulnerability;[14]
- whether the action taken to resolve or address the vulnerability was a result of a contractor-suggested recommendation;
- the date that the action taken to resolve or address the vulnerability was implemented; and
- if no action was taken to resolve or address the vulnerability, the reason why.

In addition, we conducted structured interviews with relevant CMS staff regarding the policies and procedures for handling vulnerabilities reported by PSCs, ZPICs, and MEDICs. Our questions focused on the roles of different staff in tracking, reviewing, and resolving contractor-reported vulnerabilities; procedures for tracking and reviewing vulnerability reports; and procedures for resolving reported vulnerabilities. We also reviewed all available written policies and procedures outlining how CMS tracks, reviews, and resolves contractor-reported vulnerabilities.

Data Analysis

From the vulnerability reports and information collected from CMS, we determined the number of vulnerabilities reported by each contractor. PSCs, ZPICs, and MEDICs reported a total of 70 vulnerabilities in 2009, with PSCs reporting 34 vulnerabilities, ZPICs reporting 11, and MEDICs reporting 25. For 1 of the 34 PSC-reported vulnerabilities, CMS could not find a corresponding report and, therefore, could not determine whether an actual vulnerability was reported.[15] Of the 25 MEDIC-reported vulnerabilities, CMS determined that 5 were not actual vulnerabilities and 2 were outside the scope of CMS's

[14] This included actions taken by contractors as a result of discussions and collaboration with CMS.

[15] In CMS ARTS, a vulnerability report was noted as submitted, but it is unknown whether this report identified any vulnerabilities because no corresponding vulnerability report was attached to CMS ARTS or sent to the vulnerability mailbox.

responsibilities for Parts C and D. As a result, the total number of vulnerabilities used for analysis was 62.

We categorized the vulnerabilities by type and determined the number of each type of vulnerability by contractor.

We used the information collected from CMS to identify any significant actions that CMS took to resolve each reported vulnerability. We determined actions to be significant if CMS described specific steps that it took to resolve the vulnerability. We also determined CMS's actions to be significant if, as a result, a contractor took action to resolve a vulnerability (e.g., if CMS discussed the vulnerability with the contractor and approved the contractor's plan to resolve it).

The actions that we determined not to be significant were mainly steps that CMS took to review, rather than resolve, the vulnerabilities. For example, CMS provided dates and details of correspondence with contractors or other CMS components, but did not report what, if any, corrective actions were taken as a result.

Based on our analysis of CMS's description of actions taken, we determined the number of vulnerabilities that were resolved, the number for which significant actions were taken to resolve the vulnerabilities, and the number of vulnerabilities that were not resolved.

We reviewed the vulnerability narratives and reports to determine what types of recommendations contractors made to CMS to resolve the vulnerabilities. We also asked CMS to tell us whether any actions it took were the result of contractor recommendations.

Finally, we calculated the estimated monetary impact on Medicare of the contractor-reported vulnerabilities. For each vulnerability, we calculated monetary impact by using the contractor-reported actual or estimated dollars allowed, paid, overpaid, at risk, or lost as a result of the vulnerability. Because monetary impact was reported inconsistently (e.g., some contractors reported monetary impact for a certain year, whereas others reported it for a range of years; some reported it for an individual provider, whereas others reported it for a group of providers), we aggregated monetary impact regardless of how it was reported.

Limitations

We did not ask CMS for documentation of actions taken to resolve the vulnerabilities. Therefore, we did not verify that the reported actions were taken.

Standards

This study was conducted in accordance with the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency.

As of January 2011, CMS had not resolved or taken significant action to resolve 77 percent of vulnerabilities reported by contractors in 2009

PSCs, ZPICs, and MEDICs reported 62 vulnerabilities in 2009. Seventy-seven percent (48) of these had not been resolved as of January 2011, nor had CMS taken significant action to resolve them. CMS indicated that of these 48 vulnerabilities, 20 were "currently under review" and 3 required additional analysis to determine whether they were actual vulnerabilities. For the remaining 25, we determined from CMS's description that no action was taken or that the action taken was not significant.

CMS resolved or took significant actions to resolve 14 vulnerabilities

Only two vulnerabilities were resolved. According to the report for one of these vulnerabilities, no uniform guidelines were in place for contractors to calculate the monetary "loss to government" for cases of fraud and abuse. The loss to the U.S. Government is often requested by Federal law enforcement agencies and is one of the key factors considered in determining sentences for defendants found guilty of health care fraud. To resolve this vulnerability, CMS developed a methodology for contractors to use to calculate loss to government.

The other vulnerability involved payment for unnecessary home health visits to diabetic patients. CMS adopted a 10-percent cap on outlier payments for home health agencies to reduce payments for unnecessary services.[16]

CMS took significant action to resolve 12 vulnerabilities. Actions that CMS took to resolve these vulnerabilities include changing policy, conducting medical review or additional analysis of certain providers, issuing a national fraud alert, establishing edits[17], educating contractors, providing contractors with access to data, and working to implement the National Provider Identifier (NPI) number as a single identifier for prescription drug prescribers for Medicare Part D.

Table 1 shows the status of the vulnerabilities reported by PSCs, ZPICs, and MEDICs in 2009.

[16] Medicare pays home health agencies a predetermined base payment for each 60-day episode of care per beneficiary. An outlier payment is an addition or adjustment to that base payment amount to reflect unusual variation in the type or amount of medically necessary home health care.

[17] Edits—system processes that use automated logic—can be used to prevent improper claims from being paid or to flag claims for further review. Edits are a means of verifying and validating claims data and are necessary to detect errors or potential errors.

Table 1: Status of Vulnerabilities Reported by Contractors in 2009

Contractor Type	Status of Vulnerability			
	Not Resolved	Significant Actions Taken To Resolve	Resolved	Total
PSC	33	0	0	33
ZPIC	5	5	1	11
MEDIC	10	7	1	18
Total	**48**	**12**	**2**	**62**

Source: OIG analysis of the status of vulnerabilities reported to CMS in 2009.

Over half of contractors' reports regarding vulnerabilities included detailed recommendations for CMS to resolve the vulnerabilities. However, many of the significant actions that CMS took to resolve vulnerabilities were not the result of these contractor recommendations. One of the recommendations was that CMS mandate periodic reviews of home health agency cost reports to determine the true cost of providing home health services. For 9 of the 14 vulnerabilities for which CMS took action, the actions it took were not those recommended by contractors.

Coding and/or billing vulnerabilities were the most commonly reported type of vulnerabilities

Over half of the vulnerabilities reported by PSCs and ZPICs related to coding and/or billing. Some examples include: a claims processing system allowed certain claims to be paid based on incorrect codes, nonphysician practitioners inappropriately billed for services, and providers billed more than the allowed number of services.

The vulnerabilities most commonly reported by MEDICs were those related to provider identifiers. Examples include use of provider identifiers of deceased providers and use of invalid provider identifiers to bill Medicare.

Table 2 shows the number of each type of vulnerability reported by each contractor.

Table 2: Types of Vulnerabilities Reported by Contractor

Vulnerability Type	Contractor Type			
	PSC	ZPIC	MEDIC	Total
Coding/Billing	20	6	1	27
Lack of Medicare Guidelines	4	2	3	9
Provider Enrollment	5	2	0	7
Provider Identifiers	1	0	5	6
Beneficiary-Related	2	0	3	5
Data Systems/Claims Processing	1	1	2	4
Procedure/Process	0	0	2	2
Marketing Violations	0	0	2	2
Total	**33**	**11**	**18**	**62**

Source: OIG analysis of vulnerabilities reported by CMS's benefit integrity contractors in 2009.

Contractors reported monetary impact for only one-third of vulnerabilities, but their estimated impact was $1.2 billion

Only 21 of the 62 vulnerabilities reviewed had an associated monetary impact reported by the contractor. According to CMS staff, PSCs and ZPICs are required to report monetary impact in their vulnerability reports. However, less than half of the vulnerabilities submitted by PSCs and ZPICs in 2009 had an associated monetary impact reported by the contractor. MEDICs are not required to report monetary impact, and few of the vulnerabilities reported by MEDICs had reports containing this information.

For these 21 vulnerabilities, the estimated monetary impact reported was $1.2 billion, with the monetary impact of individual vulnerabilities ranging from $77,692 to $803,025,113.[18] None of these vulnerabilities had been fully resolved as of January 2011.

[18] To determine monetary impact, we aggregated estimates of overpayments, dollars at risk, and dollars lost as reported by contractors. The estimated amount is not necessarily the impact during a 1-year period. Because monetary impact was not reported for the same years or timeframes by contractors—some contractors reported monetary impact for a single year, whereas others reported monetary impact for a range of years—we aggregated all monetary impact regardless of time.

For 4 of the 21 vulnerabilities with reported monetary impact, CMS has taken significant actions to resolve the vulnerabilities, but has yet to fully resolve them. Two of these vulnerabilities had the highest amounts of reported monetary impact ($803 million and $99 million), and both involve Part D provider identifiers. The vulnerability with the reported monetary impact of $803 million involved invalid prescriber identifiers. According to the vulnerability report, between January 1, 2006, and June 24, 2009, Medicare paid a total of $803,025,113 for claims submitted using the top five prescriber identifiers, although none were bona fide identifiers. To address vulnerabilities with Part D provider identifiers, CMS is working to implement use of a single identifier, the NPI, in the prescriber ID field of the prescription drug event (PDE) data.[19] CMS also stated that it will implement edits in the Drug Data Processing System (DDPS) to resolve these vulnerabilities, but that these edits will be not be implemented until 2012.[20]

Although CMS has taken significant action to resolve the 2 vulnerabilities with the largest monetary impacts, the estimated monetary impact for the 17 vulnerabilities that (as of January 2011) had not been resolved or for which significant action had not been taken is $202 million.

Monetary impact was not reported consistently

Some contractors estimated the monetary impact by analyzing the data of an individual provider, whereas others analyzed data from a select sample of providers. Some reported monetary impact for a certain year, whereas others reported monetary impact for a range of years. Because we aggregated monetary impact regardless of time period or provider sample, the actual monetary impact of these vulnerabilities could be significantly greater than the estimated $1.2 billion.

[19] Prescription drug plans submit PDE data to CMS for prescriptions filled under Medicare Part D. The PDE record contains prescription drug cost and payment data. Among the data fields included in this record is the prescriber identifier number. Currently, prescribers can enter into this field any of the following: NPI, Unique Physician Identification Number, State license number, or Drug Enforcement Administration number.

[20] PDE data are processed in DDPS. Edits in DDPS evaluate incoming PDE data and confirm that the PDE data are valid.

Although CMS has recently begun developing procedures to consistently track and review vulnerabilities, it lacks procedures to ensure that they are resolved

All three CMS divisions responsible for tracking and reviewing vulnerabilities have procedures that outline the steps they take to track and review vulnerabilities. Although contractors have been submitting vulnerability reports since at least 2007, CMS did not begin developing these procedures until June 2010. Furthermore, only one of these divisions has developed procedures to follow up on the implementation of corrective actions to resolve vulnerabilities.

CMS has begun developing new procedures to track and review vulnerabilities

Currently, each CMS division responsible for tracking and reviewing PSC-, ZPIC-, and MEDIC-reported vulnerabilities has its own tracking system and procedures for reviewing vulnerabilities. Two divisions review PSC- and ZPIC-reported vulnerabilities: one division reviews vulnerabilities involving improper payments, and the other tracks all vulnerabilities but takes the lead on tracking vulnerabilities involving fraud, waste, and abuse. PSCs and ZPICs have been submitting vulnerability reports since at least 2008; however, it was not until 2010 that these two CMS divisions developed their own procedures for handling PSC- and ZPIC-reported vulnerabilities.

A third CMS division is responsible for tracking and reviewing MEDIC-reported vulnerabilities. Although MEDICs have been reporting vulnerabilities quarterly since at least 2007, this CMS division only recently began drafting standard operating procedures to address the reported vulnerabilities and to delineate the roles and responsibilities of division staff in this process. It also did not have a system to track MEDIC-reported vulnerabilities until February 2011.

CMS is developing a centralized vulnerability tracking system, the Program Vulnerability Tracking System (PVTS). Once it becomes operational, PVTS will enable all three CMS divisions to track vulnerabilities. Contractors also will be able to directly submit their vulnerability reports into PVTS.

Not all CMS divisions have procedures to ensure that vulnerabilities are resolved

In most cases, the CMS divisions responsible for tracking and reviewing vulnerabilities are not responsible for taking direct action to resolve

them. Instead, division staff refer vulnerabilities to other CMS components that have authority to take corrective action.

For the MEDIC-reported vulnerabilities, CMS division staff stated that because they are not directly involved with resolving vulnerabilities, they do not routinely keep track of corrective actions implemented to resolve them. For some of these MEDIC-reported vulnerabilities, division staff must coordinate with other components within CMS that take action for resolution. Division staff stated that in these cases, corrective actions are recorded once the resolution has been implemented (e.g., regulatory language has been changed or a system change has been made). However, division staff do not have procedures for routinely following up to determine whether vulnerabilities have been resolved.

Similarly, the CMS division responsible for tracking and reviewing PSC- and ZPIC-reported vulnerabilities does not have procedures for following up to ensure that vulnerabilities have been resolved. Once a vulnerability is referred to the appropriate CMS component, the division considers the status of the vulnerability to be "closed."

The division responsible for reviewing PSC- and ZPIC-reported vulnerabilities involving improper payments across the Medicare program has developed a standard operating protocol for tracking the implementation of corrective actions. However, these procedures do not establish timeframes for following up with the CMS components to ensure prompt resolution of vulnerabilities.

RECOMMENDATIONS

One of the ways that Medicare benefit integrity contractors help prevent fraud, waste, and abuse is by identifying program vulnerabilities. To minimize the financial impact on Medicare, CMS needs to take prompt action to resolve vulnerabilities. Only two of the vulnerabilities reported in 2009 had been resolved as of January 2011. Given that the estimated monetary impact of vulnerabilities reported in 2009 was over a billion dollars, millions of dollars may continue to be at risk each year if vulnerabilities are not being promptly and effectively resolved.

It is also important that vulnerabilities' monetary impact be consistently reported and tracked. For most of the vulnerabilities in 2009, contractors did not report monetary impact. When contractors did report monetary impact, it was not reported consistently. Because monetary impact is often used to prioritize vulnerabilities needing corrective action, the consistent reporting of monetary impact will ensure that CMS has all the necessary information to make informed decisions about resolving vulnerabilities. None of the vulnerabilities with reported monetary impact have been resolved, although CMS has taken significant action to resolve the two with the greatest monetary impact ($803 million and $99 million). However, implementation of these actions will not be complete until 2012, 3 years after the vulnerabilities were reported.

To gain sufficient oversight of program vulnerabilities, CMS needs to have policies and procedures for ensuring the prompt resolution of vulnerabilities. Contractors have been reporting vulnerabilities for several years; however, CMS has not been conducting routine followup to determine whether corrective actions have been taken to resolve the reported vulnerabilities. In 2011, CMS was still reviewing vulnerabilities reported in 2008 and 2009 to determine whether they had been resolved or whether action still needed to be taken to resolve them.

Therefore, we recommend that CMS:

Determine the status of all vulnerabilities that have not been resolved and take action to address them

CMS needs to promptly follow up on the vulnerabilities reported in 2009 that have not been resolved. CMS needs to determine what actions, if

any, have been taken to resolve them in the 2 years since they were reported.

Require all benefit integrity contractors to report monetary impact, when calculable, in a consistent format

PSCs and ZPICs have been required to report vulnerabilities for several years. According to CMS staff, PSCs and ZPICs were required to submit vulnerability reports using a revised report template beginning in December 2010. This revised template includes the amount of estimated or actual dollars at risk, if known. MEDICs are not required to report monetary impact. CMS should ensure that PSCs, ZPICs, and MEDICs report actual or estimated monetary impact whenever possible. However, when it would be too burdensome or time consuming to estimate monetary impact, contractors should still report the vulnerability and explain why the calculation of monetary impact was not possible. Additionally, to accurately assess vulnerabilities' monetary impact on Medicare and to more effectively prioritize the actions needed, CMS should develop a consistent way for benefit integrity contractors to report this impact. For example, CMS should request that when possible contractors report monetary impact for a standard timeframe, such as 1 year.

Ensure that vulnerabilities are resolved by establishing formal written procedures that include timeframes for followup and that outline CMS and contractor responsibilities regarding vulnerability resolution

Because contractors and different CMS components are involved in resolving vulnerabilities, coordination is essential for prompt resolution. CMS needs to establish formal written procedures that include timeframes for following up with contractors and other involved CMS components to ensure that vulnerabilities are resolved promptly. Procedures should also include specific roles and responsibilities of CMS and contractors in ensuring that vulnerabilities are resolved.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

CMS acknowledged the importance of identifying vulnerabilities in preventing fraud, waste, and abuse. CMS also acknowledged the importance of minimizing the financial impact on Medicare by taking prompt action to resolve vulnerabilities. CMS concurred with our first recommendation and is determining the status of all open vulnerabilities and taking action, when possible, to address them. CMS

stated that it has determined the status of all vulnerabilities identified by the MEDICs.

CMS did not concur with our second recommendation. CMS stated that it would be challenging to require all benefit integrity contractors to report the monetary impact for each vulnerability and to use it in a consistent methodology. CMS noted that it could be labor intensive for the contractors to determine the dollars at risk for vulnerabilities and that not all vulnerabilities have a monetary impact that results in a loss to the Medicare Trust Fund. Furthermore, CMS states that different types of vulnerabilities would require different methods of calculating or estimating the monetary impact or would even make such a determination impossible or very difficult because of the time and resources required. We understand that calculating the monetary impact for some vulnerabilities may not be possible. We also understand that different types of vulnerabilities would require different methods of calculating monetary impact. However, for cases in which calculating the monetary impact is too burdensome or time consuming, the contractor should report the vulnerabilities and explain why the monetary impact could not be calculated. Based on CMS' comments, we clarified the wording of this recommendation.

CMS concurred in part with our third recommendation. CMS stated that it has standard operating procedures in place and continues to actively manage reported vulnerabilities on a monthly basis. CMS stated that it can establish timeframes for resolution on a case-by-case basis, but said that it will be difficult to establish standard timeframes because actions and resolutions to address vulnerabilities will vary. Although we agree that actions and resolutions vary depending on the type of vulnerability, it is possible to have standard timeframes for following up to determine the status of the vulnerabilities. Standard intervals, such as every 6 months, for following up with the various CMS components and staff responsible for addressing vulnerabilities would ensure that vulnerabilities are being appropriately and promptly addressed, regardless of the specific actions and resolutions that are implemented.

The full text of CMS's comments is provided in the Appendix.

APPENDIX

Agency Comments

DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

Administrator
Washington, DC 20201

DATE: OCT 26 2011

TO: Daniel R. Levinson
Inspector General

/S/

FROM: Donald M. Berwick, M.D.
Administrator

SUBJECT: Office of Inspector General (OIG) Draft Report: "Addressing Vulnerabilities Reported by Medicare Benefit Integrity Contractors" (OEI-03-10-00500)

The Centers for Medicare & Medicaid Services (CMS) appreciates the opportunity to review and comment on the Office of Inspector General (OIG) draft report entitled, "Addressing Vulnerabilities Reported by Medicare Benefit Integrity Contractors." This report had multiple objectives. First, it seeks to determine whether CMS resolved vulnerabilities reported by Medicare benefit integrity contractors. Secondly, it determined the monetary impact of the reported vulnerabilities on the Medicare program, and lastly, the report reviews CMS' procedures for tracking, reviewing, and resolving reported vulnerabilities.

One of the ways that Medicare program integrity contractors help prevent fraud, waste, and abuse is by identifying program vulnerabilities. To minimize the financial impact of these vulnerabilities on the Medicare program, CMS needs to take prompt action to resolve them. CMS currently has vulnerability standard operating procedures in place and continues to actively manage reported vulnerabilities on a monthly basis. CMS is collaborating and coordinating throughout the Agency to address program vulnerabilities, as appropriate. We note that CMS cannot always resolve the vulnerabilities or resolve them as promptly as CMS would like due to various constraints. For example, the magnitude and complexity of the resolution, such as changing a regulation or requesting a system change, may require significant time to resolve the vulnerability. Additionally, some vulnerabilities require legislative changes to resolve.

We appreciate the OIG's efforts in working with CMS to help ensure that vulnerabilities are addressed. Our response to each of the OIG recommendations and other comments follow.

OIG Recommendation

Determine the status of all vulnerabilities that have not been resolved and take action to address them.

CMS Response

The CMS concurs with this recommendation and is in the process of addressing OIG's recommendation. CMS is currently in the process of determining the status of all open vulnerabilities and taking action, when possible, to address them. CMS has determined the status of all vulnerabilities identified by the Medicare drug integrity contractors.

As mentioned in the OIG report, CMS cannot always resolve the vulnerabilities or resolve them as promptly as CMS would like due to various constraints. For example, the magnitude and complexity of the resolution, such as changing a regulation or requesting a system change, may require significant time to resolve the vulnerability. Additionally, some vulnerabilities require statutory changes to resolve.

OIG Recommendation

Require all benefit integrity contractors to report monetary impact in a consistent format.

CMS Response

The CMS does not concur with this recommendation. In some cases, CMS may be able to determine the monetary impact; however, requiring all benefit integrity contractors to report the monetary impact for each vulnerability and use it in a consistent methodology would prove challenging for two main reasons.

First, if in the course of performing research and investigation the contractor identifies the dollars at risk, this information can be provided. Otherwise, it is likely to be labor intensive to identify and extrapolate the dollars at risk for vulnerabilities. It may be a better use of Agency resources to address a vulnerability versus determining the precise monetary impact. In addition, not all vulnerabilities have a monetary impact that result in a loss to the Trust Fund (e.g., policy vulnerabilities). For example, there may be vulnerabilities identified that affect quality of care but do not change what CMS would have paid for items or services rendered under a bundled or capitated payment system.

Secondly, different types of vulnerabilities, e.g., provider enrollment versus billing/coding errors, would require different methods of calculating or estimating the monetary impact or even make this determination impossible or very difficult due to the time and resources required. For example, determining the monetary impact of a provider enrollment vulnerability would be very difficult given the Agency would need to calculate cost avoidance from allowing a provider into the program. It is unclear how such costs could be determined and whether they would be accurate. In addition, calculating a monetary impact for Parts C and D vulnerabilities would be difficult, because plans are paid on a capitated basis.

OIG Recommendation

Ensure that vulnerabilities are resolved by establishing formal written procedures that include timeframes for follow-up and that outline CMS and contractor responsibilities regarding vulnerability resolution.

CMS Response

The CMS concurs in part with this recommendation. CMS currently has vulnerability standard operating procedures in place and continues to actively manage reported vulnerabilities on a monthly basis. Upon review, CMS can establish timeframes for resolution on a case-by-case basis; however, it will be difficult to establish standard timeframes, since the resolution(s) and action(s) required for each vulnerability will vary. CMS will collaborate and coordinate throughout the Agency to address program vulnerabilities, as appropriate.

Other Comments

a) Page ii of the report: "CMS did not develop these procedures until late 2010 and early 2011, after this study began."

CMS Response: The Medicare Program Integrity Group established a vulnerabilities workgroup in June 2010. Starting in June 2010, this workgroup first began developing procedures to track incoming vulnerability reports, identify the component(s) that may be able to resolve the vulnerability issue(s) and track the responses from the component(s).

b) Page 4 of the report: "CMS staff stated that PSCs and ZPICs are also required to include monetary impact in these reports."

CMS Response: The first standardized request that the ZPICs and PSCs report the monetary impact of a vulnerability came about in January 2011, which is when CMS issued a new vulnerability report template to the contractors. From that point, the PSCs and ZPICs were directed to report the monetary impact of a vulnerability when possible.

c) Page 5 of the report incorrectly describes tracking and reviewing responsibilities. The Division of Data Analysis (DDA) within the Office of Financial Management **is not currently** responsible for tracking or monitoring vulnerabilities reported by PSCs and ZPICs.

The Division of Data Analysis was created in February 2009 within the Provider Compliance Group (PCG). The PCG oversees the Comprehensive Error Rate Testing (CERT) program, the Payment Error Rate Measurement (PERM) program, the FFS Recovery Auditors, and the medical review function at the Medicare Administrative Contractors (MACs).

From February 2009 through April 11, 2010, the DDA/PCG was responsible **only** for tracking insights from the PSCs/ZPICs received through the vulnerability mailbox. These insights (or leads) were not always considered "vulnerabilities." The Program Integrity Group (PIG) was responsible for oversight (including resolution of vulnerabilities) of the PSCs/ZPICs during this time. When the vulnerability mailbox was first created (2008

through February 2009) the Division of Data Analysis/Program Integrity Group was responsible for monitoring it.

The Center for Program Integrity was created in April 11, 2010, and assumed tracking of PSC/ZPIC input and oversight.

Currently, the DDA with the Provider Compliance Group of OFM is responsible for tracking vulnerabilities reported by the Medicare FFS Recovery Auditors.

The CMS requests the references to the Office of Financial Management's responsibility for current PSC/ZPIC oversight be removed from the report.

Again, we appreciate the opportunity to comment on this draft report and look forward to working with OIG on this and other issues.

ACKNOWLEDGMENTS

This report was prepared under the direction of Robert A. Vito, Regional Inspector General for Evaluation and Inspections in the Philadelphia regional office, and Linda M. Ragone, Deputy Regional Inspector General.

Maria Schepise Johnson served as the team leader for this study. Other principal Office of Evaluation and Inspections staff from the Philadelphia regional office who contributed to the report include Courtney Hilts. Central office staff who contributed include Scott Manley.

Office of Inspector General

http://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.