Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

REVIEW OF MEDICARE ADMINISTRATIVE CONTRACTOR INFORMATION SECURITY PROGRAM EVALUATIONS FOR FISCAL YEAR 2016

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

Gloria L. Jarmon
Deputy Inspector General
for Audit Services

February 2018
A-18-17-11300

Office of Inspector General

https://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.

Notices

THIS REPORT IS AVAILABLE TO THE PUBLIC
at https://oig.hhs.gov

Section 8M of the Inspector General Act, 5 U.S.C. App., requires that OIG post its publicly available reports on the OIG Web site.

OFFICE OF AUDIT SERVICES FINDINGS AND OPINIONS

The designation of financial or management practices as questionable, a recommendation for the disallowance of costs incurred or claimed, and any other conclusions and recommendations in this report represent the findings and opinions of OAS. Authorized officials of the HHS operating divisions will make final determination on these matters.

Report in Brief
Date: February 2018
Report No. A-18-17-11300

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
OFFICE OF INSPECTOR GENERAL

Review of Medicare Administrative Contractor Information Security Program Evaluations for Fiscal Year 2016

Why OIG Did This Review

The Social Security Act requires that each Medicare administrative contractor (MAC) have its information security program evaluated annually by an independent entity. The Centers for Medicare & Medicaid Services (CMS) contracted with PricewaterhouseCoopers (PwC) to evaluate information security programs at the MACs, using a set of agreed-upon procedures (AUPs). The HHS OIG must submit to Congress annual reports on the results of these evaluations, to include assessments of their scope and sufficiency. This report fulfills that responsibility for fiscal year 2016.

Our objectives were to assess the scope and sufficiency of evaluations of CMS's MAC information security programs and to report the results of those evaluations.

How OIG Did This Review

We reviewed PwC's working papers to determine whether PwC sufficiently addressed all areas required by the AUPs. We also determined whether all security-related weaknesses were included in the PwC reports by comparing supporting documentation with the reports. We determined whether all gaps in the PwC reports were adequately supported by comparing the reports with the PwC working papers.

What OIG Found

PwC's evaluations of the contractor information security programs were adequate in scope and sufficiency. PwC reported a total of 145 gaps at the 8 MACs for FY 2016, which was 8 percent more than the number of gaps for the same 8 contractors in FY 2015; however, the number of high- and medium-risk gaps decreased. Deficiencies remain in all of the Federal Information Security Management Act of 2002 control areas tested, including high- and medium-risk gaps repeated from the previous year. CMS should continue its oversight visits and ensure that the MACs remediate all gaps in a timely manner.

What OIG Recommends and CMS Comments

This report contains no recommendations. CMS provided a technical comment, which we addressed. CMS had no other comments on the draft report.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS REVIEW

The Social Security Act (the Act), as modified by the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA), requires that each Medicare administrative contractor (MAC) have its information security program evaluated annually by an independent entity. These evaluations must address the eight major requirements enumerated in the Federal Information Security Management Act of 2002 (FISMA). The Act also requires evaluations of the information security controls for a subset of systems but does not specify the criteria for these evaluations. The Inspector General, Department of Health and Human Services, must submit to Congress annual reports on the results of these evaluations, to include assessments of their scope and sufficiency. This report fulfills that responsibility for fiscal year (FY) 2016.

OBJECTIVES

Our objectives were to assess the scope and sufficiency of MAC information security program evaluations and report the results of those evaluations.

BACKGROUND

The Medicare Program

The Centers for Medicare & Medicaid Services (CMS) administers Medicare. Medicare is a health insurance program for people age 65 or older, people under age 65 with certain disabilities, and people of all ages with end-stage renal disease. In FY 2016, Medicare paid approximately $566 billion on behalf of more than 57 million Medicare beneficiaries. CMS contracts with MACs to administer Medicare benefits paid on a fee-for-service basis. In FY 2016, eight distinct entities served as MACs for Medicare Parts A and B to process and pay Medicare fee-for-service claims.

Medicare Prescription Drug, Improvement, and Modernization Act of 2003

The MMA added information security requirements for MACs to section 1874A of the Act. (See 42 U.S.C. § 1395kk-1.) Each MAC must have its information security program evaluated annually by an independent entity (the Act § 1874A(e)(2)(A)). This section requires that these evaluations address the eight major requirements enumerated in FISMA. (See 44 U.S.C. § 3544(b).) These requirements, referred to as "FISMA control areas" in this report, are:

1. periodic risk assessments;

2. policies and procedures to reduce risk;

3. system security plans;

4. security awareness training;

5. periodic testing of information security controls;

6. remedial actions;

7. incident detection, reporting, and response; and

8. continuity of operations for information technology (IT) systems.

CMS added a ninth area for testing starting in FY 2015:

9. privacy.

Section 1874A(e)(2)(A)(ii) of the Act requires that the effectiveness of information security controls be tested for an appropriate subset of MACs' information systems. However, this section does not specify the criteria for evaluating these security controls.

Additionally, section 1874A(e)(2)(C)(ii) of the Act requires us to submit to Congress annual reports on the results of such evaluations, including assessments of their scope and sufficiency.

CMS Evaluation Process for Fiscal Year 2016

CMS developed agreed-upon procedures (AUPs) for the program evaluation on the basis of the requirements of section 1874A(e)(1) of the Act, FISMA, information security policy and guidance from the Office of Management and Budget and the National Institute of Standards and Technology (NIST), and the Government Accountability Office's (GAO) *Federal Information Systems Controls Audit Manual* (FISCAM). In FY 2016, the independent auditors, PricewaterhouseCoopers (PwC), under contract with CMS, used the AUPs to evaluate the information security programs at the eight entities that served as MACs. Two of the entities had multiple contracts with CMS to fulfill their responsibilities as Medicare Parts A and B MACs, and durable medical equipment MACs. As a result, PwC issued 10 separate reports.

To comply with the section 1874A(e)(2)(A)(ii) requirement to test the effectiveness of information security controls for an appropriate subset of contractors' information systems, CMS included in the scope of its AUP evaluations testing of segments of the Medicare claims processing systems hosted at the Medicare data centers, which support each of the MACs. Medicare data centers are used for "front-end" preprocessing of claims received from providers and "back-end" issuing of payments to providers after claims have been adjudicated.

The results of the MAC information security program evaluations are presented in terms of gaps, which are defined as a MAC's incomplete implementation of FISMA or CMS core security requirements. PwC categorized gaps into three categories: high, medium, and low risk. CMS does not require corrective action plans for low-risk gaps involving a MAC's internal controls

and its operations. The MACs are responsible for developing a corrective action plan for each high- and medium-risk gap, and CMS is responsible for tracking all corrective action plans and ensuring that such gaps are remediated in a timely manner.

CMS and PwC perform at least one oversight visit to each MAC during the year to address gaps identified by PwC during the prior year's reviews.

HOW WE CONDUCTED THIS REVIEW

We evaluated the FY 2016 results of the independent evaluations of the MACs' information security programs. Our review did not include an evaluation of internal controls.

We conducted this performance audit in accordance with generally accepted government auditing standards, except that we did not obtain comments from PwC. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix A contains the details of our audit scope and methodology.

FINDINGS

PwC's evaluations of the contractor information security programs were adequate in scope and sufficiency. At the 8 MACs in FY 2016, PwC identified a total of 145 gaps, of which 16 were high-risk gaps, 30 were medium-risk gaps, and 99 were low-risk gaps.

ASSESSMENT OF SCOPE AND SUFFICIENCY

PwC's evaluations of the MAC information security programs adequately encompassed in scope and sufficiency the nine control areas reviewed.

RESULTS OF EVALUATIONS ON MEDICARE ADMINISTRATIVE CONTRACTOR INFORMATION SECURITY PROGRAMS

As shown in Table 1, PwC identified a total of 145 gaps at the 8 MACs. The number of gaps by contractor ranged from 10 to 30 and averaged 18. See Appendix B for a list of gaps per FISMA control area by contractor.

Table 1: Range of Medicare Administrative Contractor Gaps, FYs 2015 and 2016

			Number of Contractors With				
FY	Number of Contractors	Total Gaps	0 Gaps	1–5 Gap(s)	6–10 Gaps	11–15 Gaps	16+ Gaps
2015	8	133	0	0	0	4	4
2016	8	145	0	0	1	3	4

The total number of gaps reported for the 8 MACs that PwC evaluated increased by 9 percent in FY 2016 (from 133 in FY 2015 to 145 in FY 2016). The number of MACs with 10 or less increased by 1, the number of MACs with 11 to 15 gaps decreased by 1, and the number of MACs with 16 or more gaps stayed the same. Four MACs had fewer gaps in FY 2016 and four MACs had more gaps. See Appendix C for the FY 2015 to FY 2016 percentage change in gaps per MAC.

Table 2 summarizes the gaps found in each FISMA control area in FYs 2015 and 2016. Five of the nine FISMA control areas tested in FY 2015 and FY 2016 had an increase in gaps for FY 2016, with an increase of two to seven gaps.

Table 2: Gaps by Federal Information Security Management Act Control Area in FY 2016

FISMA Control Area	No. of Gaps Identified		No. of Contractors With One or More Gap(s)	
	FY 2015	FY 2016	FY 2015	FY 2016
Periodic risk assessments	3	1	3	1
Policies and procedures to reduce risk	41	39	8	8
System security plans	14	18	8	8
Security awareness training	6	3	5	2
Periodic testing of information security controls	37	44	8	8
Remedial actions	1	3	1	3
Incident detection, reporting, and response	11	14	7	8
Continuity of operations for IT systems	9	15	5	7
Privacy	11	8	7	5
Total	**133**	**145**		

At the 8 MACs in FY 2016, PwC identified a total of 145 gaps, of which 16 were high-risk gaps, 30 were medium-risk gaps, and 99 were low-risk gaps. Of the 46 high- and medium-risk gaps, 13 (28 percent) were repeat gaps from FY 2015. In many instances, controls that were tested with similar findings from the previous year were considered repeat findings. Ten of the thirteen repeat gaps (77 percent) were identified as high risk in both FYs, of which 8 repeats were in the area of periodic testing of information security controls. Four of the ten high-risk repeat gaps were at one MAC.

The MAC information security program evaluations covered several subcategories within each FISMA control area. Individual gaps were assigned an overall risk level on a subjective basis by PwC after considering the impact on CMS and likelihood of occurrence.

The following sections discuss the three FISMA control areas containing the most gaps. See Appendix D for descriptions of each subcategory tested for the three FISMA control areas.

Periodic Testing of Information Security Controls

The effectiveness of information security policies, procedures, practices, and controls should be tested and evaluated at least annually (NIST Special Publication (SP) 800-53, Control CA-2). Security testing enables organizations to measure levels of compliance in areas such as patch management, password policy, and configuration management (NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*, section 2.3). Changes to an application should be tested and approved before being put into production (FISCAM, section 3.3).

All eight MACs had from four to seven gaps each related to periodic testing of information security controls. In total, 44 gaps were identified in this area. Following are examples of these gaps:

- Change management procedures were not consistently enforced.
- System security configurations did not comply with CMS requirements.
- Security weaknesses were found by internal network penetration testing.

Without a comprehensive program for periodically testing and monitoring information security controls, management has no assurance that appropriate safeguards are in place to mitigate identified risks.

Policies and Procedures To Reduce Risk

According to NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*:

> The selection and specification of security controls for an information system is accomplished as part of an organization-wide information security program for the management of risk—that is, the risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation of information systems. Risk-based approaches to security control selection and specification consider effectiveness, efficiency, and constraints due to applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

All eight MACs had from three to seven gaps each related to policies and procedures to reduce risk. In total, PwC identified 39 gaps in this area. Following are examples of these gaps:

- Malicious software protection mechanisms were not fully configured in a manner consistent with CMS requirements.

- Security policies and procedures over platform patch management should have been enhanced.[1]

- Policies and procedures related to external information systems connections did not meet CMS requirements.

Ineffective policies and procedures to reduce risk could jeopardize an organization's mission, information, and IT assets. Without adequate configuration standards and the latest security patches, systems may be susceptible to exploitation that could lead to unauthorized disclosure of data, data modification, or the unavailability of data.

System Security Plans

An agency should ensure that its information security policy is sufficiently current to accommodate the information security environment and the agency mission and operational requirements (NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, section 2.2.5). Organizations must screen individuals before authorizing access to information systems (NIST SP 800-53, Control PS-3); they should disable information system access immediately following an employee's termination (NIST SP 800-53, Control PS-4); and they should develop system security plans to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements (Executive Summary of NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*).

All eight MACs had from one to four gaps each related to system security plans. In total, PwC identified 18 gaps in this area. Following are examples of these gaps:

- Access control procedures were not consistently enforced.

- Policies and procedures were not reviewed within 365 days of the previous review date in accordance with CMS requirements.

- The system security plan did not reflect the current operating environment.

If information security program requirements are not implemented and enforced, management has no assurance that established system security controls will be effective in protecting

[1] A patch is a piece of software designed to correct security and functionality problems in software programs and firmware.

valuable assets, such as information, hardware, software, systems, and related technology assets that support the organization's critical missions.

OVERSIGHT REVIEWS

CMS performs at least one oversight visit to each MAC during the year to address gaps identified by PwC during the prior year's reviews, with the emphasis being on gaps across multiple MACs. During FY 2016, CMS and PwC visited each of the 8 MACs, emphasizing configuration management submissions, system security plans submissions, and MAC-specific challenging areas based on prior year findings. During future oversight reviews, more emphasis will be placed on addressing specific repeat findings, including low-risk gaps at each MAC.

CONCLUSION

The scope of the work and sufficiency of documentation for all reported gaps were sufficient for the eight MACs reviewed by PwC. While the total number of gaps, which includes low-risk gaps, identified at the MACs had increased from FY 2015, the number of high-and medium-risk gaps decreased. Deficiencies remained in all of the FISMA control areas tested, including high- and medium-risk gaps repeated from the previous year. CMS should continue its oversight visits and ensure that the MACs remediate all gaps in a timely manner.

CMS COMMENTS

CMS provided a technical comment, which we addressed. CMS had no other comments on the draft report.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We evaluated the FY 2016 results of the independent evaluations of MACs' information security programs. Our review did not include an evaluation of internal controls. We performed our reviews of PwC working papers from March through September 2017.

METHODOLOGY

To accomplish our objectives, we performed the following steps:

- To assess the scope of the evaluations of contractor information security programs, we determined whether the AUPs included the eight FISMA control areas enumerated in section 1874A(e)(1) of the Act.

- To assess the sufficiency of the evaluations of contractor information security programs, we reviewed PwC working papers supporting the evaluation reports to determine whether PwC sufficiently addressed all areas required by the AUPs. We also determined whether all security-related weaknesses were included in the PwC reports by comparing supporting documentation with the reports. We determined whether all gaps in the PwC reports were adequately supported by comparing the reports with the PwC working papers.

- To report on the results of the evaluations, we aggregated the results in the individual contractor evaluation reports. For the PwC evaluations, we used the number of gaps listed in the individual MAC evaluation reports to aggregate the results.

We conducted this performance audit in accordance with generally accepted government auditing standards, except that we did not obtain comments from PwC. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

APPENDIX B: GAPS BY FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002 CONTROL AREA AND MEDICARE ADMINISTRATIVE CONTRACTOR IN FISCAL YEAR 2016

	Control Areas									
MAC	**Periodic Risk Assessments**	**Policies and Procedures To Reduce Risk**	**System Security Plans**	**Security Awareness Training**	**Periodic Testing of Information Security Controls**	**Remedial Actions**	**Incident Detection, Reporting, and Response**	**Continuity of Operations for IT Systems**	**Privacy**	**Total Gaps**
1	0	7	4	2	7	0	3	4	3	30
2	0	4	2	0	5	0	2	1	0	14
3	0	4	3	0	5	1	1	1	1	16
4	0	6	2	0	7	1	3	4	1	25
5	0	4	1	0	4	0	1	0	0	10
6	0	3	2	1	5	1	1	1	0	13
7	0	4	1	0	4	0	2	2	2	15
8	1	7	3	0	7	0	1	2	1	22
Total	**1**	**39**	**18**	**3**	**44**	**3**	**14**	**15**	**8**	**145**

APPENDIX C: PERCENTAGE CHANGE IN GAPS PER MEDICARE ADMINISTRATIVE CONTRACTOR, FISCAL YEARS 2015 AND 2016

MAC	FY 2015 Gaps	FY 2016 Gaps	% Change
1	25	30	20
2	15	14	(7)
3	15	16	7
4	17	25	47
5	16	10	(38)
6	14	13	(7)
7	17	15	(12)
8	14	22	57
Total	**133**	**145**	**9%**

APPENDIX D: RESULTS OF MEDICARE ADMINISTRATIVE CONTRACTOR EVALUATIONS FOR FEDERAL INFORMATION SECURITY MANAGEMENT ACT OF 2002 CONTROL AREAS WITH THE GREATEST NUMBER OF GAPS

PERIODIC TESTING OF INFORMATION SECURITY CONTROLS

The evaluations of the MAC information security program covered seven subcategories related to the periodic testing of information security controls. The evaluation reports identified a total of 44 gaps in this FISMA control area.

Table 3: Gaps in the Area of Periodic Testing of Information Security Controls in FY 2016

	Subcategory	No. of Gaps in This Area
1	Annual reviews and audits are conducted to evaluate compliance with FISMA guidance from the Office of Management and Budget for reviews of IT security controls, including platform configuration standards.	8
2	Change control management procedures exist.	3
3	Change control procedures are tested by management to make certain they are in use.	6
4	Systems are configured according to the contractor's documented security configuration checklists.	8
5	Weaknesses are identified by PwC during a network attack and penetration test.	8
6	A formally maintained system component inventory is up to date and accurate.	5
7	The provider Internet portal is compliant with section 508 of the Rehabilitation Act of 1973.	6
	Total	**44**

POLICIES AND PROCEDURES TO REDUCE RISK

The evaluations of the MAC information security program assessed nine subcategories related to policies and procedures to reduce risk. The evaluation reports identified a total of 39 gaps in this FISMA control area.

Table 4: Gaps in the Area of Policies and Procedures To Reduce Risk in FY 2016

	Subcategory	No. of Gaps in This Area
1	Systems security controls have been tested and evaluated. The system and network boundaries have been subjected to periodic reviews or audits. Management reports exist for review and testing of IT security policies and procedures, including network risk assessment, accreditations and certifications, internal and external audits and security reviews, and penetration and vulnerability assessments.	3
2	All gaps in compliance per CMS's minimum security requirements are identified in the results of management's compliance checklist.	0
3	Security policies and procedures include controls to address platform security configurations.	3
4	Security policies and procedures include controls to address patch management.	5
5	The latest patches have been installed on contractors' systems.	5
6	Security settings are included within internal checklists and comply with Defense Information Systems Agency standards.	8
7	Malicious software protection mechanisms have been installed on workstations and laptops, are up to date and operating effectively, and administrators are alerted of any malicious software identified on workstations and laptops.	6
8	Full-device or container encryption protect the confidentiality and integrity of information on approved mobile devices.	2
9	Strict terms and conditions for the use of external information systems to store, access, transmit, or process sensitive systems have been established.	7
	Total	**39**

SYSTEM SECURITY PLANS

The evaluations of the MAC information security program assessed six subcategories related to system security plans. The evaluation reports identified a total of 18 gaps in this FISMA control area.

Table 5: Gaps in the Area of System Security Plans in FY 2016

	Subcategory	No. of Gaps in This Area
1	A security plan is documented and approved.	1
2	The security plan is kept current.	4
3	A security management structure has been established and criticality or sensitivity risk designations have been assigned to positions.	0
4	Hiring, transfer, and termination policies address security.	5
5	Employee background checks are performed.	4
6	Management has documented that it periodically assesses the appropriateness of security policies and compliance with these.	4
	Total	**18**