Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

REVIEW OF MEDICARE ADMINISTRATIVE CONTRACTOR INFORMATION SECURITY PROGRAM EVALUATIONS FOR FISCAL YEAR 2019

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

Amy J. Frontz
Deputy Inspector General
for Audit Services

August 2020
A-18-20-11300

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 audits 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 website.

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: August 2020
Report No. A-18-20-11300

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

Review of Medicare Administrative Contractor Information Security Program Evaluations for Fiscal Year 2019

Why OIG Did This Audit

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 Guidehouse, LLP (Guidehouse), to evaluate information security programs at the MACs, using a set of agreed-upon procedures (AUPs). 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 (FY) 2019.

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

How OIG Did This Audit

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

What OIG Found

Guidehouse's evaluations of the contractor information security programs were adequate in scope and sufficiency. Guidehouse reported a total of 125 gaps at the 7 MACs for FY 2019, which was 12 percent more than the number of gaps for the same 7 contractors in FY 2018. The increase was due in part to the addition of database and web server testing. Deficiencies remained in each of the nine Federal Information Security Modernization Act of 2014 control areas that were tested. CMS should continue its oversight visits and ensure that the MACs remediate all gaps to improve the MACs' information technology security.

What OIG Recommends

This report contains no recommendations.

The full report can be found at https://oig.hhs.gov/oas/reports/region18/182011300.asp.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS AUDIT

The Inspector General, Department of Health and Human Services, is required to report to Congress the results of annual independent evaluations of the information security programs of Medicare administrative contractors (MACs) as required by the Social Security Act (the Act), as modified by the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA). These evaluations must address the eight major requirements enumerated in the Federal Information Security Modernization Act of 2014 (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. This report fulfills that responsibility for fiscal year (FY) 2019.

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 2019, Medicare paid approximately $657 billion on behalf of over 60 million Medicare beneficiaries. CMS contracts with MACs to administer Medicare benefits paid on a fee-for-service basis. In FY 2019, seven 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 2019

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 2019, the independent auditors, Guidehouse, LLP (Guidehouse), under contract with CMS, used the AUPs to evaluate the information security programs at the seven 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, Guidehouse issued nine 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 claim 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. Guidehouse categorized gaps into three categories: high, moderate, and low

risk. The MACs are responsible for developing a corrective action plan for each high- and moderate-risk gap, and CMS is responsible for tracking all corrective action plans and ensuring that such gaps are remediated in a timely manner. CMS does not require corrective action plans for low-risk gaps involving a MAC's internal controls and its operations, but those gaps are reviewed with the MACs during oversight visits.

CMS performs at least one oversight visit to each MAC during the year to address all gaps identified by Guidehouse during the prior year's reviews.

HOW WE CONDUCTED THIS AUDIT

We evaluated the FY 2019 results of the independent evaluations of the MACs' information security programs. We 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 Guidehouse. 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.

RESULTS

Guidehouse's evaluations of the contractor information security programs were adequate in scope and sufficiency. At the 7 MACs evaluated in FY 2019, Guidehouse identified a total of 125 gaps, of which 15 were high-risk gaps, 38 were moderate-risk gaps, and 72 were low-risk gaps.

ASSESSMENT OF SCOPE AND SUFFICIENCY

Guidehouse'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 on the next page, Guidehouse identified a total of 125 gaps at the 7 MACs for FY 2019. The number of gaps by contractor ranged from 13 to 24 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 2018 and 2019

			Number of Contractors With:				
FY	Number of Contractors	Total Gaps	0 Gaps	1–5 Gap(s)	6–10 Gaps	11–15 Gaps	16+ Gaps
2018	7	112	0	0	0	3	4
2019	7	125	0	0	0	2	5

The total number of gaps reported for the 7 MACs that Guidehouse evaluated increased by 12 percent in FY 2019 (from 112 in FY 2018 to 125 in FY 2019). The increase was due in part to new and updated testing procedures. There was no change in the number of MACs with 10 or fewer gaps, the number of MACs with 11 to 15 gaps decreased by 1, and the number of MACs with 16 or more gaps increased by 1. Three MACs had fewer gaps in FY 2019, and three MACs had more gaps. See Appendix C for the FY 2018 to FY 2019 percentage change in gaps per MAC.

Table 2 summarizes the gaps found in each FISMA control area in FYs 2018 and 2019. Two of the nine FISMA control areas tested in FY 2018 and FY 2019 had a decrease in gaps for FY 2019, with a decrease of one gap and five gaps. Six of the nine FISMA control areas tested had an increase for FY 2019, with an increase of one to six gaps. One FISMA control area tested had the same number of gaps.

Table 2: Gaps by Federal Information Security Modernization Act Control Area in FY 2019

FISMA Control Area	No. of Gaps Identified		No. of Contractors With One or More Gap(s)	
	FY 2018	FY 2019	FY 2018	FY 2019
Periodic risk assessments	1	3	1	2
Policies and procedures to reduce risk	32	31	7	7
System security plans	16	20	7	7
Security awareness training	1	1	1	1
Periodic testing of information security controls	35	30	7	7
Remedial actions	1	2	1	2
Incident detection, reporting, and response	12	18	7	7
Continuity of operations for IT systems	14	19	7	7
Privacy	0	1	0	1
Total	**112**	**125**		

At the 7 MACs in FY 2019, Guidehouse identified a total of 125 gaps, of which 15 were high-risk gaps, 38 were moderate-risk gaps, and 72 were low-risk gaps. The number of high-risk gaps

increased by 15 percent (13 in FY 2018), moderate-risk gaps increased by 15 percent (33 in FY 2018), and low-risk gaps increased by 9 percent (66 in FY 2018). Guidehouse identified one repeat gap from FY 2018. It should be noted that additional controls were tested in FY 2019. In many instances, controls that were tested had similar findings from the previous year but were not considered repeat findings by Guidehouse because some of the gaps were the result of database and web server testing in the current year.

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 Guidehouse 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.

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 seven MACs had four to five gaps each related to policies and procedures to reduce risk. In total, Guidehouse identified 31 gaps in this area. Following are examples of these gaps:

- Systems operating in the contractor's environment did not have the latest patches installed.[1]

- Security configuration checklists did not comply with CMS requirements.

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

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

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.

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 seven MACs had from three to five gaps each related to periodic testing of information security controls. In total, 30 gaps were identified in this area. Following are examples of these gaps:

- System component inventory processes had not been implemented in accordance with CMS requirements.

- System security configurations did not comply with CMS requirements.

- Security weaknesses were identified as part of the internal network penetration test.

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.

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 seven MACs had from two to four gaps each related to system security plans. In total, Guidehouse identified 20 gaps in this area. Following are examples of these gaps:

- The system security plan did not reflect the current operating environment.
- Access control policies and procedures were not consistently enforced.
- Background investigation policies and procedures were not documented in accordance with CMS Business Partner System Security Manual requirements.

If information security program requirements are not implemented and enforced, management has no assurance that established system security controls will be effective in protecting 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 Guidehouse during the prior year's reviews and to improve the logical security of its systems and control of the MAC's security program and computer operations. During FY 2019, CMS visited each of the seven MACs and reviewed selected MAC controls and operations for cybersecurity, emphasizing configuration management, log review, firewall rules review, and MAC-specific challenging areas based on prior-year findings.

CONCLUSION

The scope of the work and sufficiency of documentation for all reported gaps were sufficient for the seven MACs reviewed by Guidehouse. The total number of gaps identified at the MACs had increased significantly from FY 2018, in part because of the expanded testing. Deficiencies remained in each of the nine FISMA control areas tested. CMS should continue its oversight visits and ensure that the MACs remediate all gaps to improve the MACs' IT security. Similar gaps from prior years should be considered repeat findings to highlight the existence of continued exposure to known weaknesses.

This report contains no recommendations.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We evaluated the FY 2019 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 Guidehouse working papers from March through May 2020.

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

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

We provided CMS with a draft audit report on July 9, 2020, for review. CMS had no written comments.

We conducted this performance audit in accordance with generally accepted government auditing standards, except that we did not obtain comments from Guidehouse. 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 MODERNIZATION ACT OF 2014 CONTROL AREA AND MEDICARE ADMINISTRATIVE CONTRACTOR IN FISCAL YEAR 2019

	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	5	3	0	5	0	3	4	0	20
2	0	4	2	0	4	0	2	1	0	13
3	1	5	3	0	3	1	2	2	0	17
4	2	4	4	1	4	0	4	5	0	24
5	0	4	2	0	4	0	2	1	0	13
6	0	5	3	0	5	0	3	1	1	18
7	0	4	3	0	5	1	2	5	0	20
Total	**3**	**31**	**20**	**1**	**30**	**2**	**18**	**19**	**1**	**125**

APPENDIX C: CHANGE IN GAPS PER MEDICARE ADMINISTRATIVE CONTRACTOR, FISCAL YEARS 2018 AND 2019

MAC	FY 2018 Gaps	FY 2019 Gaps	# Change	% Change
1	18	20	2	11
2	14	13	(1)	(7)
3	18	17	(1)	(6)
4	12	24	12	100
5	14	13	(1)	(7)
6	16	18	2	13
7	20	20	0	0
Total	**112**	**125**	**13**	**12%**

APPENDIX D: RESULTS OF MEDICARE ADMINISTRATIVE CONTRACTOR EVALUATIONS FOR FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 CONTROL AREAS WITH THE GREATEST NUMBER OF GAPS

POLICIES AND PROCEDURES TO REDUCE RISK

The evaluations of the MAC information security program assessed ten subcategories related to policies and procedures to reduce risk. The evaluation reports identified a total of 31 gaps in this FISMA control area.

Table 3: Gaps in the Area of Policies and Procedures To Reduce Risk in FY 2019

	Subcategory	No. of Gaps in This Area
1	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 assessments.	0
2	Results of management's compliance reviews with the CMS Acceptable Risk Safeguards.	0
3	Security policies and procedures include controls to address platform security configurations.	7
4	Security policies and procedures include controls to address patch management.	7
5	The latest patches have been installed on contractors' systems.	5
6	Security settings are included within checklists and comply with Defense Information Systems Agency standards.	7
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.	2
8	Organization maintains an approved software whitelist and enforces the whitelist with both preventative and detective controls.	2
9	Organization employs full-device or container encryption to protect the confidentiality and integrity of information on approved mobile devices.	0

	Subcategory	No. of Gaps in This Area
10	Organization implements data protection mechanisms that prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.	1
	Total	**31**

PERIODIC TESTING OF INFORMATION SECURITY CONTROLS

The evaluations of the MAC information security program covered nine subcategories related to the periodic testing of information security controls. The evaluation reports identified a total of 30 gaps in this FISMA control area.

Table 4: Gaps in the Area of Periodic Testing of Information Security Controls in FY 2019

	Subcategory	No. of Gaps in This Area
1	Configuration management processes are performed in accordance with CMS requirements.	6
2	Change control management procedures exist.	1
3	Change control procedures are tested by management to make certain they are in use.	0
4	Systems are configured according to the contractor's documented security configuration checklists.	7
5	Weaknesses are identified by Guidehouse during a network attack and penetration test.	7
6	A formally maintained system component inventory is up to date and accurate.	3
7	The organization's Internet portal is compliant with section 508 of the Rehabilitation Act of 1973.	3
8	The organization has implemented email and web browser protections.	2
9	Wireless network access controls exist.	1
	Total	**30**

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 20 gaps in this FISMA control area.

Table 5: Gaps in the Area of System Security Plans in FY 2019

	Subcategory	No. of Gaps in This Area
1	A security plan is documented, approved, and kept current.	7
2	A security management structure has been established, and criticality or sensitivity risk designations have been assigned to positions.	0
3	Hiring, transfer, and termination policies and procedures address security.	3
4	Organization follows documented procedures on hired, transferred, and terminated employees and contractors.	4
5	Employee background checks are performed.	4
6	Management has documented that it periodically assesses the appropriateness of security policies and compliance with these.	2
	Total	**20**