Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

REVIEW OF MEDICARE ADMINISTRATIVE CONTRACTOR INFORMATION SECURITY PROGRAM EVALUATIONS FOR FISCAL YEAR 2023

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

September 2024
A-18-24-11300

Office of Inspector General

https://oig.hhs.gov

The mission of the Office of Inspector General (OIG) is to provide objective oversight to promote the economy, efficiency, effectiveness, and integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of the people they serve. Established by Public Law No. 95-452, as amended, OIG carries out its mission through audits, investigations, and evaluations conducted by the following operating components:

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. The audits examine the performance of HHS programs, funding recipients, and contractors in carrying out their respective responsibilities and provide independent assessments of HHS programs and operations to reduce waste, abuse, and mismanagement.

Office of Evaluation and Inspections. OEI's national evaluations provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. To promote impact, OEI reports also provide practical recommendations for improving program operations.

Office of Investigations. OI's criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs and operations often lead to criminal convictions, administrative sanctions, and civil monetary penalties. OI's nationwide network of investigators collaborates with the Department of Justice and other Federal, State, and local law enforcement authorities. OI works with public health entities to minimize adverse patient impacts following enforcement operations. OI also provides security and protection for the Secretary and other senior HHS officials.

Office of Counsel to the Inspector General. OCIG provides legal advice to OIG on HHS programs and OIG's internal operations. The law office also imposes exclusions and civil monetary penalties, monitors Corporate Integrity Agreements, and represents HHS's interests in False Claims Act cases. In addition, OCIG publishes advisory opinions, compliance program guidance documents, fraud alerts, and other resources regarding compliance considerations, the anti-kickback statute, and other OIG enforcement authorities.

REPORT HIGHLIGHTS

September 2024 | A-18-24-11300

Review of Medicare Administrative Contractor Information Security Program Evaluations for Fiscal Year 2023

Why OIG Did This Audit

- The Social Security Act requires each Medicare administrative contractor (MAC) to have its information security program evaluated annually by an independent entity.
- CMS contracted with Guidehouse, LLP, to evaluate information security programs at seven, MACs using a set of agreed-upon procedures. OIG must submit to Congress annual reports on the results of these evaluations and include assessments of their scope and sufficiency. This report fulfills that responsibility for fiscal year (FY) 2023.
- This audit assessed the scope and sufficiency of MAC information security program evaluations.

What OIG Found

- Guidehouse's evaluations of MACs' information security programs were adequate in scope and sufficiency. A total of 94 gaps at the 7 MACs were identified in FY 2023, which was a 2 percent increase in the number of gaps identified for the same 7 MACs in FY 2022. The number of high- and moderate-risk gaps increased by 19 percent from FY 2022. Deficiencies occurred in eight of the nine Federal Information Security Modernization Act of 2014 control areas that were tested.
- The results warrant CMS to continue its oversight visits to ensure that the MACs remediate all gaps to improve information technology security, especially those MACs for which there was an increase in the number of gaps identified compared to the previous year. Similar gaps identified in different systems being tested should be noted as systemic problems that result in continued exposure to known weaknesses.

What OIG Recommends

This report contains no recommendations.

CMS had no written comments on our draft report.

TABLE OF CONTENTS

INTRODUCTION

WHY WE DID THIS AUDIT

The Social Security Act (the Act), as modified by the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA), requires the Department of Health and Human Services, Office of Inspector General (OIG), to report to Congress the results of annual independent evaluations of the information security programs of Medicare administrative contractors (MACs). 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) 2023.

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 2023, Medicare paid approximately $868 billion on behalf of approximately 66 million Medicare enrollees. CMS contracts with MACs to administer Medicare benefits paid on a fee-for-service basis. In FY 2023, 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. systems 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 OIG 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 2023

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's) *Federal Information Systems Controls Audit Manual* (FISCAM). In FY 2023, the independent auditors, Guidehouse, LLP, 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 testing of Medicare claim processing systems hosted at the Medicare data centers. 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 operations, but those gaps are reviewed with the MACs during oversight visits.

CMS conducted in-person site visits at 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 2023 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 OF AUDIT

Guidehouse's evaluations of the contractor information security programs were adequate in scope and sufficiency. At the 7 MACs evaluated in FY 2023, a total of 94 gaps, of which 8 were high-risk gaps, 29 were moderate-risk gaps, and 57 were low-risk gaps. The number of high- and moderate-risk gaps increased by 19 percent from FY 2022.

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 OF MEDICARE ADMINISTRATIVE CONTRACTOR INFORMATION SECURITY PROGRAMS

As shown in Table 1 on the next page, Guidehouse identified a total of 94 gaps at the 7 MACs in FY 2023. The number of gaps identified at each contractor ranged from 9 to 16 and averaged 13. See Appendix B for a list of gaps per FISMA control area by contractor.

Table 1: Range of Medicare Administrative Contractor Gaps, FYs 2022 and 2023

FY	Number of Contractors	Total Gaps	Number of Contractors With: 0–10 Gaps	11–15 Gaps	16+ Gaps
2022	7	92	2	3	2
2023	7	94	2	3	2

The total number of gaps reported for the 7 MACs that Guidehouse evaluated increased by 2 percent in FY 2023 (from 92 in FY 2022 to 94 in FY 2023). One MAC had the same number of gaps in both FYs 2022 and 2023; three other MACs had fewer gaps in FY 2023, and three MAC had more gaps. See Appendix C for the FY 2022 to FY 2023 changes in gaps per MAC.

Table 2 (below) summarizes the number of gaps identified by each FISMA control area in FYs 2022 and 2023 and the number of contractors with one or more gaps in FY 2022 or FY 2023. From FY 2022 to FY 2023, there was a reduction of gaps reported in three of the nine FISMA control areas. The Policies and Procedures to Reduce Risk control area had the largest reduction of reported gaps, decreasing by six. Five FISMA control areas had increases in reported gaps between FY 2022 and FY 2023, with The System Security Plans control area having the largest increase (five). One FISMA control area (Periodic Testing of Information Security Controls) had the same number of reported gaps in FY 2022 and FY 2023. Between FY 2022 and FY 2023, there was a net increase of two gaps across the nine FISMA control areas.

Table 2: Gaps by FISMA Control Area, FYs 2022 and 2023

FISMA Control Area	No. of Gaps Identified		No. of Contractors With One or More Gap(s)	
	FY 2022	FY 2023	FY 2022	FY 2023
Periodic Risk Assessments	0	2	0	2
Policies and Procedures to Reduce Risk	34	28	7	7
Systems Security Plans	6	11	3	6
Security Awareness Training	0	2	0	2
Periodic Testing of Information Security Controls	33	33	7	7
Remedial Actions	0	1	0	1
Incident Detection, Reporting, and Response	11	13	7	7
Continuity of Operations for IT Systems	6	4	5	2
Privacy	2	0	2	0
Total	**92**	**94**		

At the 7 MACs in FY 2023, Guidehouse identified a total of 94 gaps, of which 8 were high-risk gaps, 29 were moderate-risk gaps, and 57 were low-risk gaps. The number of high-risk gaps

increased by 14 percent (from 7 in FY 2022 to 8 in FY 2023), moderate-risk gaps increased by 21 percent (from 24 in FY 2022 to 29 in FY 2023), and low-risk gaps decreased by 7 percent (from 61 in FY 2022 to 57 in FY 2023). Guidehouse did not report any repeat gaps from FY 2022. In many instances, controls tested in FY 2023 had similar findings from the prior year but were not considered repeat findings by Guidehouse because some of the gaps resulted from different systems being tested.

The MAC information security program evaluations covered several subcategories within each FISMA control area. Guidehouse assigned individual gaps an overall risk level on a subjective basis 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 and Evaluation of the Effectiveness of IT Security Policies

According to OMB Circular A-130, "Managing Information as a Strategic Resource," on Security and Privacy Assessments:

> Agencies must ensure that periodic testing and evaluation of the effectiveness of information security and privacy policies, procedures, and practices are performed with a frequency depending on risk, but at least annually.

All seven MACs had three to seven gaps related to periodic testing and evaluation of the effectiveness of information security policies. In total, Guidehouse identified 33 gaps in this area. Examples of these gaps included:

- Security weaknesses were identified during internal penetration testing.
- System security configurations did not comply with CMS requirements.
- Platforms that were noncompliant with CMS requirements for configuration management processes.

Without effective security controls and a comprehensive program for periodically testing, monitoring, and ensuring that information security controls are operating as required, management has limited assurance that appropriate safeguards are in place to minimize identified risks.

Policies and Procedures to Reduce Risk

According to NIST SP 800-53, Revision 5, Risk Management:

> Organizations must exercise *due diligence* (*emphasis* in original) in managing information security and privacy risk. This is accomplished, in part, by establishing a comprehensive risk management program that uses the flexibility inherent in NIST publications to categorize systems, select and implement security and privacy controls that meet mission and business needs, assess the effectiveness of the controls, authorize the systems for operation, and continuously monitor the systems. Exercising due diligence and implementing robust and comprehensive information security and privacy risk management programs can facilitate compliance with applicable laws, regulations, executive orders, and governmentwide policies.

All seven MACs had three to five gaps, each of which related to policies and procedures to reduce risk. In total, Guidehouse identified 28 gaps in this area. Examples of these gaps included:

- Supply Chain Risk Management processes did not comply with CMS requirements.
- Data Loss Prevention mechanisms and documentation did not comply with CMS requirements.
- Security Configuration Checklists did not comply with CMS requirements.

When supply chain risk management processes are noncompliant with CMS requirements, system vulnerabilities (including zero-day attacks[1]) could be exploited by cyber attackers to breach the networks and cause harm to organizations and society.

Incident Detection, Reporting, and Response

According to NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide:*

> Organizations should ensure that incident response policies and procedures and business continuity processes are in sync; and have a formal, focused, and coordinated approach to responding to incidents, including an incident response plan that provides the roadmap for implementing the incident response capability. Each organization needs a plan that meets its unique requirements,

[1] A zero-day attack is the use of a zero-day exploit to cause damage to or steal data from a system affected by a vulnerability. The term "Zero-Day" is used when security teams are unaware of their software vulnerability, and they've had "0" days to work on a security patch or an update to fix the issue.

which relates to the organization's mission, size, structure, and functions. The plan should lay out the necessary resources and management support. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services.

All seven MACs had one to four gaps related to incident detection, reporting, and response. In total, Guidehouse identified 13 gaps in this area. Examples of these gaps included:

- Incident management processes were not clearly defined and enforced.
- Log review policies and procedures were not documented in accordance with *CMS Business Partner System Security Manual* requirements.
- Vulnerability scan results were not being ingested into the Security Information and Event Management tool.

Effective incident response can minimize extensive damage to systems and networks, including the exfiltration or compromise of data. Well-defined and implemented log review processes are critical to responding to an attack. Without adequate implementation of log review processes, which may reveal potential security incidents, entities may miss the opportunity to proactively detect anomalies indicative of a security incident.

OVERSIGHT REVIEWS

CMS performs at least one oversight review per year of each MAC to address gaps identified by Guidehouse. During FY 2023, CMS conducted in-person site visits at each of the seven MACs and reviewed documentation of selected MAC controls and operations for cybersecurity, emphasizing supply chain controls, information location requirements, cloud risk management, and firewall configurations.

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 increased from FY 2022. Deficiencies were identified in eight of the nine FISMA control areas tested. The results warrant CMS continuing its oversight visits to ensure that the MACs remediate all gaps to improve the MACs' IT security, especially those with an increased number of gaps from the prior year. Similar gaps identified in different systems being tested should be noted as systemic problems that result in continued exposure to known weaknesses.

This report contains no recommendations.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We evaluated the FY 2023 results of the independent evaluations of the MACs' information security programs. Our review did not include an evaluation of internal controls. We performed our reviews of Guidehouse working papers from February through July 2024.

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 as well as a ninth control area added in FY 2015 by CMS for testing and privacy.

- 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 September 4, 2024, 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 FISMA CONTROL AREA AND MEDICARE ADMINISTRATIVE CONTRACTOR IN FISCAL YEAR 2023

	Control Areas									
MAC	**Periodic Risk Assessments**	**Policies and Procedures To Reduce Risk**	**Systems 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	1	3	1	1	3	0	1	0	0	10
2	0	5	2	0	5	0	2	0	0	14
3	1	3	2	0	7	0	1	2	0	16
4	0	4	0	0	5	0	4	2	0	15
5	0	5	2	0	5	0	2	0	0	14
6	0	3	1	1	3	0	1	0	0	9
7	0	5	3	0	5	1	2	0	0	16
Total	**2**	**28**	**11**	**2**	**33**	**1**	**13**	**4**	**0**	**94**

APPENDIX C: CHANGE IN GAPS PER MEDICARE ADMINISTRATIVE CONTRACTOR, FISCAL YEARS 2022 AND 2023

MAC	FY 2022 Gaps	FY 2023 Gaps	Gap Increase/Decrease	Percentage Change
1	10	10	0	0
2	18	14	(4)	(22%)
3	13	16	3	23%
4	11	15	4	36%
5	18	14	(4)	(22%)
6	10	9	(1)	(10%)
7	12	16	4	33%
Total*	**92**	**94**	**2**	

*Total percentage change: 2 percent.

APPENDIX D: RESULTS OF MEDICARE ADMINISTRATIVE CONTRACTOR EVALUATIONS FOR FISMA CONTROL AREAS WITH THE GREATEST NUMBER OF GAPS

PERIODIC TESTING AND EVALUATION OF THE EFFECTIVENESS OF IT SECURITY CONTROLS

The evaluations of the MAC information security program covered nine subcategories related to the periodic testing and evaluation of the effectiveness of IT security controls. The evaluation reports identified a total of 33 gaps in this FISMA control area. (See Table 3.)

Table 3: Gaps in the Area of Periodic Testing and Evaluation of the Effectiveness of IT Security Policies in FY 2023

	Subcategory	No. of Gaps in This Area
1	Configuration management processes are performed in accordance with CMS requirements.	7
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.	5
7	The organization's internet portal is compliant with section 508 of the Rehabilitation Act of 1973.	1
8	The organization has implemented email and web browser protections.	5
9	Wireless network access controls exist.	0
	Total	**33**

POLICIES AND PROCEDURES TO REDUCE RISK

The evaluations of the MAC information security program assessed 10 subcategories related to policies and procedures to reduce risk. The evaluation reports identified a total of 28 gaps in this FISMA control area. (See Table 4.)

Table 4: Gaps in the Area of Policies and Procedures To Reduce Risk in FY 2023

	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.	4
3	Security policies and procedures include controls to address platform security configurations.	2
4	Security policies and procedures include controls to address patch management.	3
5	The latest patches have been installed on contractors' systems.	1
6	Security settings are included within checklists and comply with CMS requirements and 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.	3
8	Organization maintains an approved software whitelist and enforces the whitelist with both preventative and detective controls.	3
9	Organization employs full-device or container encryption to protect the confidentiality and integrity of information on approved mobile devices.	0
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.	5
	Total	**28**

INCIDENT DETECTION, REPORTING, AND RESPONSE

The evaluations of the MAC information security program assessed six subcategories related to incident detection, reporting, and response. The evaluation reports identified a total of 13 gaps in this FISMA control area. (See Table 5.)

Table 5: Gaps in the Area of Incident Detection, Reporting, and Response in FY 2023

	Subcategory	No. of Gaps in This Area
1	Management has processes to monitor systems and the network for unusual activity and/or intrusion attempts.	1
2	Management has procedures to take and has taken action in response to unusual activity, intrusion attempts, and actual intrusions, including reporting.	1
3	Management incident response processes and procedures are documented in accordance with CMS requirements.	4
4	Log review policies and procedures for IT platforms that support contractor operations are documented in accordance with CMS requirements.	7
5	Log review results are evaluated for the completion of documented procedures.	0
6	Processes exist to analyze and correlate audit records across different repositories.	0
	Total	**13**