Department of Health and Human Services
Office of Inspector General
Office of Audit Services

December 2025 | OAS-25-18-064

Audit of Medicare Administrative Contractor Information Security Program Evaluations for Fiscal Year 2024

REPORT HIGHLIGHTS

December 2025 | OAS-25-18-064

Audit of Medicare Administrative Contractor Information Security Program Evaluations for Fiscal Year 2024

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 an Independent Public Accountant (IPA) to evaluate information security programs at the MACs using a set of agreed-upon procedures. HHS OIG is required to submit an annual report to Congress on the results of these evaluations and include an assessment of their scope and sufficiency. This report fulfills that responsibility for fiscal year (FY) 2024.

What OIG Found

- The IPA's evaluations of the MAC information security programs were adequate in scope and sufficiency.
- The FY 2024 evaluations identified deficiencies in 7 of the 9 Federal Information Security Modernization Act of 2014 control areas, resulting in a total of 97 gaps across the 7 MACs.

Table: Range of Medicare Administrative Contractor Gaps, FYs 2023 and 2024

			Number of Contractors With:		
FY	Number of Contractors	Total Gaps	0–10 Gaps	11–15 Gaps	16+ Gaps
2023	7	94	2	3	2
2024	7	97	0	5	2

- In FY 2024, the number of high-risk and moderate-risk gaps decreased, while the number of low-risk gaps increased. One moderate-risk gap was recurring from FY 2023; other gaps were similar to those identified in FY 2023 but were not identified by The IPA as recurring.

Table: Changes in Number of Gaps per Risk level, FYs 2023 and 2024

Risk Level	FY 2023	FY 2024	% Change
High	8	4	-50%
Moderate	29	14	-52%
Low	57	79	+39%

- The results support the need for CMS to continue its oversight of the MACs, including CMS's site visits to address gaps and improve information technology security.

What OIG Recommends

This report contains no recommendations.

CMS received a draft version of this report and provided no written comments.

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) 2024.

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 aged 65 or older, people under the age of 65 with certain disabilities, and people of all ages with end-stage renal disease. In FY 2024, Medicare paid approximately $892 billion on behalf of approximately 68 million Medicare enrollees.[1] CMS contracts with MACs to administer Medicare benefits paid on a fee-for-service basis. In FY 2024, 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] CMS, *Fiscal Year 2024 Financial Report*, November 2024. Accessed on Oct. 8, 2025. The consolidated statement of net cost for the year ended September 30, 2024, states that Medicare hospital insurance net costs were $381 billion and Medicare supplemental medical insurance net costs were $509 billion, which totals Medicare costs of $892 billion.

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

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 2024

CMS developed agreed-upon procedures (AUPs) for the program evaluation based on 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 2024, the Independent Public Accountant (IPA), 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, the IPA 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. The gaps were categorized 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. Additionally, the IPA will report whether a gap is recurring if the gap details identified from the prior year remain the same in the current year and the MAC has not completed corrective actions specific to the root cause. If the IPA identifies a gap as recurring, it may escalate the risk because of the increased likelihood of gap exploitation.

CMS conducted in-person site visits at each MAC during the year to address all gaps identified during the prior year's reviews.

HOW WE CONDUCTED THIS AUDIT

We evaluated the FY 2024 results of the independent evaluations of the MACs' information security programs. We did not perform an evaluation of internal controls.

We conducted this performance audit in accordance with generally accepted government auditing standards. 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

The evaluations of the MACs' information security programs were adequate in scope and sufficiency. At the 7 MACs evaluated in FY 2024, the evaluations revealed a total of 97 gaps, of which 4 were high-risk gaps, 14 were moderate-risk gaps, and 79 were low-risk gaps. The number of high- and moderate-risk gaps decreased by 51 percent from FY 2023.

ASSESSMENT OF SCOPE AND SUFFICIENCY

The evaluations of the MAC information security programs adequately addressed the scope and sufficiency of the nine FISMA control areas reviewed.

RESULTS OF EVALUATIONS OF MEDICARE ADMINISTRATIVE CONTRACTOR INFORMATION SECURITY PROGRAMS

As shown in Table 1, a total of 97 gaps were identified at the 7 MACs in FY 2024. The number of gaps identified at each contractor ranged from 11 to 16 and averaged 14. See Appendix B for a list of gaps per FISMA control area by contractor.

Table 1: Range of Medicare Administrative Contractor Gaps, FYs 2023 and 2024

			Number of Contractors With:		
FY	Number of Contractors	Total Gaps	0–10 Gaps	11–15 Gaps	16+ Gaps
2023	7	94	2	3	2
2024	7	97	0	5	2

The total number of gaps reported for the 7 MACs that were evaluated increased by 3 percent in FY 2024 (from 94 in FY 2023 to 97 in FY 2024). One MAC had the same number of gaps in both FYs 2023 and 2024, one MAC had fewer gaps in FY 2024, and five MACs had more gaps. See Appendix C for the FY 2023 to FY 2024 changes in gaps per MAC.

Table 2 summarizes the number of gaps identified by each FISMA control area in FYs 2023 and 2024 and the number of contractors with gaps in FY 2023 or FY 2024. From FY 2023 to FY 2024, there was a reduction of gaps reported in two of the nine FISMA control areas. The Policies and Procedures to Reduce Risk control area had the largest reduction of reported gaps, decreasing by eight. Three FISMA control areas had increases in reported gaps between FY 2023 and FY 2024, with the Continuity of Operations for IT Systems control area having the largest increase (six). One FISMA control area (Privacy) maintained zero reported gaps, and another FISMA control area (Periodic Risk Assessments) had the same number of reported gaps in FY 2023 and FY 2024. Between FY 2023 and FY 2024, there was a net increase of four gaps across the nine FISMA control areas.

Table 2: Gaps by FISMA Control Area, FYs 2023 and 2024

FISMA Control Area	No. of Gaps Identified		No. of Contractors With One or More Gap(s)	
	FY 2023	FY 2024	FY 2023	FY 2024
Periodic Risk Assessments	2	2	2	2
Policies and Procedures to Reduce Risk	28	20	7	7
Systems Security Plans	11	15	6	7
Security Awareness Training	2	3	2	3
Periodic Testing of Information Security Controls	33	34	7	7
Remedial Actions	1	0	1	0

Incident Detection, Reporting, and Response	13	13	7	7
Continuity of Operations for IT Systems	4	10	2	5
Privacy	0	0	0	0
Total	**94**	**97**		

Table 3 summarizes the changes in the number of MAC gaps identified per risk level for the 7 MACs from FY 2023 to FY 2024.

Table 3: Changes in Number of Gaps per Risk level, FYs 2023 and 2024

Risk Level	FY 2023	FY 2024	% Change
High	8	4	-50%
Moderate	29	14	-52%
Low	57	79	+39%

One of the moderate-risk gaps was identified as recurring from FY 2023. In many instances, controls tested in FY 2024 had similar gaps from the prior year, but were not considered recurring because the gaps resulted from different systems being tested.

The MAC information security program evaluations covered several subcategories within each FISMA control area. The individual gaps were assigned a risk level on a subjective basis after considering the impact on CMS if the gap was exploited and likelihood of that 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 at Appendix 1, section 5.e:

> 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 . . .. Security and privacy control assessments shall ensure that security and privacy controls selected by agencies are implemented correctly, operating as intended, and effective in satisfying security and privacy requirements . . ..
>
> Technical security tools . . . (which look for known security weaknesses and configuration errors . . .), and penetration testing can assist in the ongoing assessment of information systems . . ..

All seven MACs had four to six gaps related to periodic testing and evaluation of the effectiveness of information security policies. In total, 34 gaps were identified in this area. Examples of these gaps included:

- Configuration management processes were not performed in accordance with CMS requirements.

- Systems were not configured according to the contractor's documented security configuration checklists.

- Security weaknesses were identified during network attack and penetration testing.

- The formally maintained system component inventory was not up to date and accurate.

Without security controls being implemented correctly, 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*, at page vi:

> Organizations must exercise due diligence 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 two to four gaps, each of which related to the policies and procedures to reduce risk control area. In total, 20 gaps were identified in this area. Examples of these gaps included:

- Security settings were not included within checklists or did not comply with CMS requirements.

- Security policies and procedures did not include controls to address patch management.

- Data loss prevention mechanisms and documentation did not comply with CMS requirements.

When organizations do not adequately manage risk and are noncompliant with CMS requirements, system vulnerabilities (including zero-day attacks)[2] could be exploited by cyber attackers to breach the networks and cause harm to organizations and society.

Systems Security Plans

According to NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems,* section 1.7 System Security Plan Responsibilities*:*

> Agencies should develop policy on the system security planning process. System security plans are living documents that require periodic review, modification, and plans of action and milestones for implementing security controls. Procedures should be in place outlining who reviews the plans, keeps the plan current, and follows up on planned security controls. In addition, procedures should require that system security plans be developed and reviewed prior to proceeding with the security certification and accreditation process for the system.

All seven MACs had one or three gaps related to systems security plans control area. In total, 15 gaps were identified in this area, one of which was recurring from FY 2023. Examples of these gaps included:

- The systems security plans were not kept current to reflect the current operating environment.

- The systems security plans included an annual recertification of accounts for hired, transferred, and terminated employees or contractors; however, five MACs did not follow documented procedures for recertification.

- The system security plan package did not include formal processes for monitoring security controls, risks, and impacts of Cloud Service Providers to ensure up-to-date information is available. (This is the recurring gap.)

Without updated security plans and the implementation of plan procedures, MAC's have limited assurance that security requirements are met and identified threats are mitigated.

OVERSIGHT REVIEWS

CMS performs at least one oversight review per year of each MAC to address gaps identified. During FY 2024, CMS conducted in-person site visits at each of the seven MACs and reviewed

[2] 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.

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 documentation for all reported gaps were sufficient for the seven MACs reviewed. The total number of gaps identified at the MACs increased from FY 2023. Deficiencies were identified in seven 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 the different tested systems should be noted as systemic problems that result in continued exposure to known weaknesses. Root-cause analysis could identify these gaps as recurring.

This report contains no recommendations.

APPENDIX A: AUDIT SCOPE AND METHODOLOGY

SCOPE

We evaluated the FY 2024 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 the IPA working papers from February through September 2025.

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

- To report on the results of the evaluations, we aggregated the results in the individual contractor evaluation reports. For the evaluations, we used the number of gaps listed in the individual MAC evaluation reports to aggregate the results. To illustrate changes in the number of gaps identified last year, we compared the results of the FY 2023 evaluations with the 2024 results.

We provided CMS with a draft audit report on November 7, 2025, for review. CMS had no written comments.

We conducted this performance audit in accordance with generally accepted government auditing standards. 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 2024

	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	0	2	3	0	5	0	2	0	0	12
2	0	4	1	1	5	0	2	2	0	15
3	1	3	3	0	6	0	2	1	0	16
4	1	2	3	1	5	0	2	2	0	16
5	0	4	1	1	5	0	2	2	0	15
6	0	2	3	0	4	0	2	0	0	11
7	0	3	1	0	4	0	1	3	0	12
Total	**2**	**20**	**15**	**3**	**34**	**0**	**13**	**10**	**0**	**97**

APPENDIX C: CHANGE IN GAPS PER MEDICARE ADMINISTRATIVE CONTRACTOR, FISCAL YEARS 2023 AND 2024

MAC	FY 2023 Gaps	FY 2024 Gaps	Gap Increase/Decrease	Percentage Change
1	10	12	+2	+20%
2	14	15	+1	+7%
3	16	16	0	0%
4	15	16	+1	+7%
5	14	15	+1	+7%
6	9	11	+2	+22%
7	16	12	-4	-25%
Total*	**94**	**97**	**+3**	

*Total percentage change: 3 percent.

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

PERIODIC TESTING OF INFORMATION 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 34 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 2024

	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.	0
3	Change control procedures are tested by management to make certain they are in use.	3
4	Systems are configured according to the contractor's documented security configuration checklists.	7
5	Weaknesses are identified during a network attack and penetration test.	7
6	A formally maintained system component inventory is up to date and accurate.	7
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.	2
9	Wireless network access controls exist.	0
	Total	**34**

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 20 gaps in this FISMA control area. (See Table 4.)

Table 4: Gaps in the Area of Policies and Procedures To Reduce Risk in FY 2024

	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.	0
4	Security policies and procedures include controls to address patch management.	4
5	The latest patches have been installed on contractors' systems.	2
6	Security settings are included within checklists and comply with CMS requirements and Defense Information Systems Agency standards.	6
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.	0
9	Organization employs full-device or container encryption to protect the confidentiality and integrity of information on approved mobile devices.	1
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.	4
	Total	**20**

SYSTEMS SECURITY PLANS

The evaluations of the MAC information security program assessed five subcategories related to system security plans. The evaluation reports identified a total of 15 gaps in this FISMA control area. (See Table 5.)

Table 5: Gaps in the Area of Systems Security Plans in FY 2024

	Subcategory	No. of Gaps in This Area
1	Evaluate if security plan is documented, approved, and kept current.	6
2	Evaluate if hiring, transfer, and termination policies and procedures address security.	1
3	Gather a selection of hired, transferred, and terminated employees and contractors to make certain that the contractor followed documented procedures.	5
4	Evaluate if employee background checks are performed.	0
5	Evaluate the cloud implementation details and documentation within the system security plan package.	3
	Total	**15**

Report Fraud, Waste, and Abuse

OIG Hotline Operations accepts tips and complaints from all sources about potential fraud, waste, abuse, and mismanagement in HHS programs. Hotline tips are incredibly valuable, and we appreciate your efforts to help us stamp out fraud, waste, and abuse.

TIPS.HHS.GOV

Phone: 1-800-447-8477

TTY: 1-800-377-4950

Who Can Report?

Anyone who suspects fraud, waste, and abuse should report their concerns to the OIG Hotline. OIG addresses complaints about misconduct and mismanagement in HHS programs, fraudulent claims submitted to Federal health care programs such as Medicare, abuse or neglect in nursing homes, and many more. Learn more about complaints OIG investigates.

How Does It Help?

Every complaint helps OIG carry out its mission of overseeing HHS programs and protecting the individuals they serve. By reporting your concerns to the OIG Hotline, you help us safeguard taxpayer dollars and ensure the success of our oversight efforts.

Who Is Protected?

Anyone may request confidentiality. The Privacy Act, the Inspector General Act of 1978, and other applicable laws protect complainants. The Inspector General Act states that the Inspector General shall not disclose the identity of an HHS employee who reports an allegation or provides information without the employee's consent, unless the Inspector General determines that disclosure is unavoidable during the investigation. By law, Federal employees may not take or threaten to take a personnel action because of whistleblowing or the exercise of a lawful appeal, complaint, or grievance right. Non-HHS employees who report allegations may also specifically request confidentiality.

Stay In Touch

Follow HHS-OIG for up to date news and publications.

 OIGatHHS

 HHS Office of Inspector General

Subscribe To Our Newsletter

OIG.HHS.GOV

Contact Us

For specific contact information, please visit us online.

U.S. Department of Health and Human Services
Office of Inspector General
Public Affairs
330 Independence Ave., SW
Washington, DC 20201

Email: Public.Affairs@oig.hhs.gov