


DEPARTMENT OF MEDICAL ASSISTANCE SERVICES

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2025

Auditor of Public Accounts
Staci A. Henshaw, CPA
www.apa.virginia.gov
(804) 225-3350

AUDIT SUMMARY

Our audit of the Department of Medical Assistance Services (Medical Assistance Services), including the Medicaid Cluster of federal grant programs, for the fiscal year ended June 30, 2025, found:

- proper recording and reporting of all transactions, in all material respects, in the Commonwealth's accounting and reporting system, Medical Assistance Services' financial systems, and supplemental information and attachments submitted to the Department of Accounts;

- two matters involving internal control and its operation requiring management's attention, that also represent instances of noncompliance with applicable laws and regulations that are required to be reported under Government Auditing Standards; however, we do not consider them to be material weaknesses; and

- adequate corrective action with respect to the prior audit findings identified as complete in the Findings Summary included in the Appendix.

Additionally, our report includes two risk alerts that require the action and cooperation of Medical Assistance Services' management and the Virginia Information Technologies Agency (VITA) regarding risks related to unpatched software and access to centralized audit log information.

In the section titled "Internal Control and Compliance Findings and Recommendations," we have included our assessment of the conditions and causes resulting in the internal control and compliance findings identified through our audit as well as recommendations for addressing those findings. Our assessment does not remove management's responsibility to perform a thorough assessment of the conditions and causes of the findings and develop and appropriately implement adequate corrective actions to resolve the findings as required by the Department of Accounts in Topic 10205 – Agency Response to APA Audit of the Commonwealth Accounting Policies and Procedures Manual. Those corrective actions may include additional items beyond our recommendation.

-TABLE OF CONTENTS–

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Improve Database Security
Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2024

The Department of Medical Assistance Services (Medical Assistance Services) has made significant progress improving security for the database supporting its primary system for financial accounting and reporting in accordance with its internal procedures, the Commonwealth's Information Security Standard, SEC530 (Security Standard), and industry best practices, such as the Center for Internet Security Benchmarks (CIS Benchmark). Since the prior year audit, Medical Assistance Services remediated four of the eight weaknesses previously identified. However, Medical Assistance Services does not define deviations from recommended and expected security configurations in its baseline configuration, leading to some weaknesses still existing in the database. We communicated the remaining weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under § 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

The Security Standard requires Medical Assistance Services to develop, document, and disseminate information security policies and procedures that align with the control requirements in the Security Standard. Additionally, the Security Standard requires Medical Assistance Services to develop, document, and maintain a current baseline configuration of the system; apply more restrictive security configurations for sensitive systems; and monitor systems for security baseline and policy compliance. Without aligning the database's settings and configurations with its policies and procedures, the Security Standard, and industry best practices, Medical Assistance Services cannot ensure data integrity within the database. Additionally, without documenting details and the justification for approved deviations, Medical Assistance Services increases the risk that it will not meet minimum-security requirements and recommendations to protect its sensitive data from malicious parties. A lack of resources led to Medical Assistance Services experiencing delays in resolving the remaining weaknesses.

Medical Assistance Services should dedicate the resources necessary to review and update its procedures to define deviations from recommended and expected security configurations as well as business justification and approval for any deviations. Additionally, Medical Assistance Services should develop a process to review the database's configuration against its established procedures on a scheduled basis and after major changes occur to help detect and address potential misconfigurations timely. Furthermore, Medical Assistance Services should implement the security controls and processes communicated in the FOIAE document to address the risks present in the database to ensure the configuration aligns with its procedures, the Security Standard, and CIS Benchmark. These actions will help maintain the confidentiality, availability, and integrity of Medical Assistance Services' sensitive and mission-critical data.

Improve IT Third-Party Oversight Process

Type: Internal Control and Compliance
Severity: Significant Deficiency
First Reported: Fiscal Year 2022

Medical Assistance Services is continuing its efforts to implement its formal process to maintain oversight for three of its information technology (IT) third-party service providers that manage and support its Medicaid management system. The Medicaid management system encompasses different functions, such as member and provider reporting, financial reporting, and federal reporting.

Medical Assistance Services has collected data since the prior audit to implement its IT Third Party Risk Management Procedure, which was effective in February 2024, and comply with its IT System and Services Acquisition Policy. However, Medical Assistance Services is still determining the best method to consistently capture the necessary data, which has resulted in the agency not yet verifying the following required controls and processes for one of the Medicaid management system IT service providers not covered by the Virginia Information Technologies Agency's (VITA) Commonwealth of Virginia Risk and Authority Management Program.

- Medical Assistance Services does not confirm the geographic location of sensitive data monthly for the IT service providers. Without confirming the geographic location of sensitive data, Medical Assistance Services may be unable to enforce contract requirements, laws, and standards due to the data falling outside the United States' jurisdiction.

- Medical Assistance Services does not confirm whether IT service providers perform vulnerability scans every 90 days. By not obtaining and analyzing the vulnerability scan results from the IT service provider, Medical Assistance Services increases the risk that the IT service providers are not remediating legitimate vulnerabilities in a timely manner.

Medical Assistance Services has required additional time to collaborate with its IT service provider to adjust its data collection methods and verification processes. Medical Assistance Services also had to prioritize its resources to remediate ongoing findings from previous audits.

Medical Assistance Services should continue its efforts to implement its IT Third Party Risk Management Procedure and ensure those tasked with monitoring IT service providers confirm the geographic location of sensitive data, the provider's performance of vulnerability scanning, and remediation efforts per the Security Standard. Medical Assistance Services should also ensure the individuals responsible for monitoring consistently perform formal oversight processes in a timely manner, which will help maintain the confidentiality, integrity, and availability of sensitive and mission-critical data.

RISK ALERTS

During our audit, we encountered issues that are beyond the corrective action of Medical Assistance Services' management alone and require the action and cooperation of management and VITA. The following issues represent such a risk to Medical Assistance Services and the Commonwealth.

Unpatched Software

First Reported: Fiscal Year 2021

VITA contracts with various providers, collectively known as the Commonwealth's Information Technology Infrastructure Services Program (ITISP), to provide agencies with installation, maintenance, operation, and support of IT infrastructure components, such as servers, routers, firewalls, and virtual private networks. Medical Assistance Services continues to rely on contractors procured by VITA for the installation of security patches in systems that support Medical Assistance Services' operations. Additionally, Medical Assistance Services relies on VITA as the contract administrator to maintain oversight and enforce the contract agreements with the ITISP contractors. As of August 2025, the ITISP contractors had not applied a significant number of security patches that are critical and highly important to Medical Assistance Services' IT infrastructure components, all of which are past the 30-day update window allowed by the Security Standard.

The Security Standard requires the installation of security-relevant software and firmware updates within 30 days of release or within a timeframe approved by VITA's Commonwealth Security and Risk Management division. The Security Standard does allow for varying time periods depending on factors such as the criticality of the update, but generally the ITISP uses a 30-day window from the date of release as its standard for determining timely implementation of security patches. Missing system security updates increase the risk of successful cyberattack, exploit, and data breach by malicious parties.

While VITA is responsible for enforcing the service level agreement, it has not been able to compel the current ITISP contractors to install certain security patches to Medical Assistance Services' IT infrastructure to remediate vulnerabilities in a timely manner or take actions to obtain these required services from another source. Medical Assistance Services is working with VITA and the ITISP contractors to ensure that the ITISP contractors install all critical and highly important security patches on all servers. Our separate audit of VITA's contract management will also continue to report this issue.

Access to Centralized Audit Log Information
First Reported: Fiscal Year 2021

Medical Assistance Services relies on the Commonwealth's ITISP to install, maintain, operate, and support IT infrastructure components, such as servers, routers, firewalls, and virtual private networks. As the ITISP contract administrator, VITA is responsible for providing agencies with access to its security information and event management (SIEM) tool that stores information about historical security events for these components that may affect Medical Assistance Services' IT environment.

VITA and the ITISP contractors implemented the current SIEM tool in October 2023 after several unsuccessful iterations since 2018. While the current SIEM tool stores audit logs for the ITISP infrastructure components, the SIEM tool does not present the information in a usable format that will allow agencies to adequately monitor their IT environments. Additionally, VITA has not configured the SIEM tool to give alerts about specific events captured in the audit logs. These alerts are necessary to provide Medical Assistance Services with timely notification of potentially anomalous or malicious activity.

The Security Standard requires agencies to review and analyze audit records at least every 30 days for indications of inappropriate or unusual activity and assess any potential impact of the inappropriate or unusual activity. Using a SIEM tool without all necessary audit log information displayed to agencies reduces organizational security posture by not being able to react to and investigate suspicious system activity in a timely manner.

Medical Assistance Services should continue to work with VITA to create relevant and usable information on the SIEM tool, including setting the appropriate alerts, to ensure Medical Assistance Services can review the activities occurring in its IT environment in accordance with the Security Standard. Our separate audit of VITA's contract management will also continue to report this issue.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 15, 2025

The Honorable Glenn Youngkin
Governor of Virginia

Joint Legislative Audit
and Review Commission

Janet Kelly
Secretary of Health and Human Resources

Cheryl J. Roberts
Director, Department of Medical Assistance Services

We have audited the financial records, operations, and federal compliance of the **Department of Medical Assistance Services** (Medical Assistance Services), including the Medicaid Cluster of federal grant programs, for the year ended June 30, 2025. We conducted this audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, in support of the Commonwealth's Annual Comprehensive Financial Report and Single Audit. 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.

Audit Objectives

Our audit's primary objective was to evaluate the accuracy of Medical Assistance Services' financial transactions as reported in the Annual Comprehensive Financial Report for the Commonwealth of Virginia and test federal compliance in support of the Commonwealth's Single Audit for the year ended June 30, 2025. In support of this objective, we evaluated the accuracy of recorded financial transactions in the Commonwealth's accounting and financial reporting system, Medical Assistance Services' financial systems, and supplemental information and attachments submitted to the Department of Accounts; reviewed the adequacy of Medical Assistance Services' internal control; tested for compliance with applicable laws, regulations, contracts, and grant agreements; and reviewed corrective actions with respect to audit findings from prior year reports.

Audit Scope and Methodology

Medical Assistance Services' management has responsibility for establishing and maintaining internal control and complying with applicable laws, regulations, contracts, and grant agreements. Internal control is a process designed to provide reasonable, but not absolute, assurance regarding the reliability of financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws, regulations, contracts, and grant agreements.

We gained an understanding of the overall internal controls, both automated and manual, sufficient to plan the audit. We considered materiality and risk in determining the nature and extent of our audit procedures. Our review encompassed controls over the Medicaid Cluster of federal grant programs and the following significant cycles, classes of transactions, and account balances:

Accounts payable
Accounts receivable
Contract procurement and management
Federal revenues, expenses, and compliance for the Medicaid Cluster
General Fund revenues (drug rebates) and expenses
Information system security (including access controls)
Provider assessment revenues and expenses

We performed audit tests to determine whether Medical Assistance Services' controls were adequate, had been placed in operation, and were being followed. Our audit also included tests of compliance with provisions of applicable laws, regulations, contracts, and grant agreements. Our audit procedures included inquiries of appropriate personnel, inspection of documents, records, and contracts, and observation of Medical Assistance Services' operations. We performed analytical procedures, including budgetary and trend analyses, and tested details of transactions to achieve our audit objectives.

A nonstatistical sampling approach was used. Our samples were designed to support conclusions about our audit objectives. An appropriate sampling methodology was used to ensure the samples selected were representative of the population and provided sufficient, appropriate evidence. We identified specific attributes for testing each of the samples and, when appropriate, we projected our results to the population.

Our consideration of internal control over financial reporting and federal compliance (internal control) was for the limited purpose described in the section "Audit Objectives" and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We identified certain deficiencies in internal control titled "Improve Database Security" and "Improve IT Third-Party Oversight Process," which are described in the section

titled "Internal Control and Compliance Findings and Recommendations," that we consider to be significant deficiencies.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements or noncompliance on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements or material noncompliance with a type of compliance requirement of a federal program will not be prevented or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Conclusions

We found that Medical Assistance Services properly stated, in all material respects, the amounts recorded and reported in the Commonwealth's accounting and financial reporting system, Medical Assistance Services' financial systems, and supplemental information and attachments submitted to the Department of Accounts.

We noted certain matters involving internal control and its operation and compliance with applicable laws, regulations, contracts, and grant agreements that require management's attention and corrective action. These matters are described in the section titled "Internal Control and Compliance Findings and Recommendations."

Medical Assistance Services has taken adequate corrective action with respect to prior audit findings identified as complete in the Findings Summary included in the Appendix.

Since the findings noted above include those that have been identified as significant deficiencies, they will be reported as such in the "Independent Auditor's Report on Internal Control over Financial Reporting and on Compliance and Other Matters Based on an Audit of the Financial Statements Performed in Accordance with Government Auditing Standards" and the "Independent Auditor's Report on Compliance for Each Major Federal Program; Report on Internal Control over Compliance; and Report on Schedule of Expenditures of Federal Awards Required by Uniform Guidance," which are included in the Commonwealth of Virginia's Single Audit Report for the year ended June 30, 2025. The Single Audit Report will be available at www.apa.virginia.gov in February 2026.

Exit Conference and Report Distribution

We discussed this report with management at an exit conference held on January 16, 2026. Government Auditing Standards require the auditor to perform limited procedures on Medical Assistance Services' response to the findings identified in our audit, which is included in the

accompanying section titled "Agency Response." Medical Assistance Services' response was not subjected to the other auditing procedures applied in the audit and, accordingly, we express no opinion on the response.

This report is intended for the information and use of the Governor and General Assembly, management, and the citizens of the Commonwealth of Virginia and is a public record.

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

JDE/vks

FINDINGS SUMMARY

Finding Title	Status of Corrective Action*	Fiscal Year First Reported
Improve Information Security Program and Controls	Complete	2020
Improve Fiscal Agent Oversight	Complete	2024
Improve Vulnerability Remediation Efforts	Complete	2024
Improve Database Security	Ongoing	2024
Improve IT Third-Party Oversight Process	Ongoing	2022

* A status of **Complete** indicates management has taken adequate corrective action. A status of **Ongoing** indicates new and/or existing findings that require management's corrective action as of fiscal year end.

COMMONWEALTH of VIRGINIA

Department of Medical Assistance Services

CHERYL J. ROBERTS
DIRECTOR

SUITE 1300
600 EAST BROAD STREET
RICHMOND, VA 23219
804/786-7933
804/343-0634 (TDD)
www.dmas.virginia.gov

January 16, 2026

Ms. Staci A. Henshaw, CPA
Auditor of Public Accounts
Commonwealth of Virginia
P. O. Box 1295
Richmond, Virginia 23218

Dear Ms. Henshaw:

We have reviewed the FY24 Audit Report for the Department of Medical Assistance Services (DMAS) for the Fiscal Year Ending June 30, 2025. We concur with the audit findings and will submit a response to the Department of Accounts, within the required thirty days after the report is issued. The response will include the work plans for corrective actions that DMAS will take to address the audit findings.

We appreciate the audit team's work and feedback. If you have any questions or require additional information, please contact the DMAS Internal Audit Director, Susan Smith.

Sincerely,

Cheryl J. Roberts
Director