AGENCIES OF THE SECRETARY OF HEALTH AND HUMAN RESOURCES

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2017

Auditor of Public Accounts
Martha S. Mavredes, CPA
www.apa.virginia.gov
(804) 225-3350

AUDIT SUMMARY

This report summarizes our fiscal year 2017 audit results for the following four agencies under the Secretary of Health and Human Resources. Collectively these four agencies spent $13.4 billion or 95 percent of the total expenses for agencies under this secretariat.

- *Department of Behavioral Health and Developmental Services*
- *Department of Health*
- *Department of Medical Assistance Services*
- *Department of Social Services*

Our audits of these agencies arise from our work on the Commonwealth's Comprehensive Annual Financial Report and Single Audit of federal funds. Overall, we found the following:

- proper recording and reporting of all transactions, in all material respects, in the Commonwealth's accounting and financial reporting system, each agency's accounting records, and other financial information reported to the Department of Accounts;

- twenty-eight findings involving internal control and its operation, necessary to bring to management's attention. Of these findings, five are considered to be material weaknesses at the Department of Medical Assistance Services;

- twenty-seven out of the twenty-eight findings are also considered to be instances of non-compliance with applicable laws and regulations that are required to be reported; and

- twelve out of the twenty-eight findings are matters not adequately resolved from the previous year that are repeated in this report. One of these is a partial repeat meaning that some progress had been made since our previous report.

–TABLE OF CONTENTS–

Pages

AUDIT SUMMARY

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Department of Behavioral Health and Developmental Services 1-16

Department of Health 17-20

Department of Medical Assistance Services 21-36

Department of Social Services 37-42

INDEPENDENT AUDITOR'S REPORT 43-47

AGENCY RESPONSES

Department of Behavioral Health and Developmental Services 48-51

Department of Health 52

Department of Medical Assistance Services 53-68

Department of Social Services 69

AGENCY OFFICIALS 70

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

This section is organized by agency and each finding reported includes information on the type of finding and the severity classification for the finding. The severity classifications are discussed in more detail in the section titled "Independent Auditor's Report." In addition, those findings that report on issues that were not resolved from our previous audit and are repeated in this report are also designated.

Department of Behavioral Health and Developmental Services

Why the APA Audits Information Systems Security

The Department of Behavioral Health and Developmental Services (DBHDS) collects, manages, and stores significant volumes of personal and financial data within its mission critical systems. Because of the highly sensitive and critical nature of this data, DBHDS management must take all necessary precautions to ensure the integrity and security of the data within its systems. To determine if information technology governance, database security, oversight of sensitive systems, and contingency management was adequate, we compared the practices of DBHDS to those required by the Commonwealth's Information Security Standard.

Continue to Improve IT Governance

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes

Condition

DBHDS is making progress to improve their information technology (IT) governance, but still has an insufficient governance structure to effectively protect sensitive Commonwealth data in accordance with the Commonwealth's standards and manage its information security program. DBHDS has a decentralized IT environment that allows the Central Office and 15 separate facilities to manage and maintain sensitive systems independently. Historically, facilities had the ability to develop and implement their own applications. The facilities also manage their own information security programs with limited resources and very little collaboration with other facilities and Central Office. This resulted in non-enterprise and redundant applications and inconsistent implementation of requirements in the Commonwealth's Information Security Standard (Security Standard), SEC501-09.

Due to the decentralized IT environment, DBHDS still has over 200 disparate sensitive systems at the Central Office and facilities, with multiple systems performing the same or similar business functions. For example, there are currently four pharmacy management systems including the electronic health records system. DBHDS intends this system to be an enterprise solution; however, only three facilities

are using it, and there is no formal timetable to implement the electronic health records system at the other facilities because DBHDS lacks the IT resources and funding.

DBHDS began the Facility Application Inventory Reduction (FAIR) project last year to reduce the number of applications across the facilities and improve their IT governance program. DBHDS is working with an external consultant to develop a roadmap and determine the resources necessary to complete the project. Due to a lack of resources and funding, DBHDS anticipates the project will take several years.

DBHDS continues to make progress and reduce the total number of sensitive systems but still has over 200 sensitive systems. This significant number of sensitive systems requires extensive IT resources to ensure compliance with the agency's enterprise security program and the Security Standard. While DBHDS is developing the FAIR project, the Central Office is implementing processes to ensure facilities are not implementing more non-enterprise and redundant applications. For example, Central Office now reviews and approves all IT procurements at the facilities. This gives Central Office the ability to deny a potential IT procurement or funds the facilities could use to implement a new application.

Criteria

Agency heads are responsible for ensuring that a sufficient information security program is maintained, documented, and effectively communicated to protect the agency's IT systems (Security Standard, Section 2.4.2).

In addition, DBHDS continues to have control weaknesses in the following areas, showing that DBHDS still lacks the necessary resources to maintain appropriate oversight over its information security program and to not meet the requirements in the Security Standard;

- End-of-life technology (Security Standard, Section SI-2-COV)
- Software baseline configurations (Security Standard, Section CM-2)
- Contingency management program (Security Standard, Section CP-1)
- Assurance over third-party providers (Security Standard, Section 1.1)

Consequence

Not having an appropriate governance structure to properly manage the agency's IT environment and information security program can result in a data breach or unauthorized access to confidential and mission critical data leading to data corruption, data loss, or system disruption if accessed by a malicious attacker, either internal or external. If a breach occurs and Health Insurance Portability and Accountability Act (HIPAA) data is stolen, the agency can incur large penalties, as much as $1.5 million.

Cause

DBHDS has a decentralized IT governance structure, which originally led to them having 437 disparate sensitive systems they could not properly manage and maintain. Today, the total number of sensitive systems is significantly less; however, DBHDS lacks the necessary IT resources at the Central Office and facilities to ensure compliance with the requirements in the Security Standard and enterprise security program. Additionally, the current reporting structure is not conducive for coordinating IT efforts between the Central Office and the facilities.

Recommendation

DBHDS should continue to consolidate their disparate sensitive systems to a level where the current IT resources can maintain compliance with the Security Standard and agency policies or hire additional resources to do so. DBHDS should evaluate its governance structure to determine the most efficient and productive method to bring the Central Office and the facilities in compliance with the requirements in the Security Standard. DBHDS should also evaluate its IT resource levels to ensure sufficient resources are available to implement the FAIR project. Implementing these recommendations will help ensure the confidentiality, integrity, and availability of DBHDS' sensitive data.

Improve IT Contingency Management Program
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Condition

DBHDS does not have complete processes or governance structure to manage and maintain their contingency management program. A contingency management program consists of an IT Continuity of Operations Plan (COOP) and a Disaster Recovery Plan (DRP).

Specifically, DBHDS does not define roles and responsibilities to ensure the IT COOP and DRP plans are consistent across the Central Office and facilities. DBHDS has hospitals, mental health institutes, and training centers that manage their own mission critical IT applications that help provide patient services. Three of these facilities do not have an IT COOP, one facility and the Central office do not have a DRP, and the remaining facilities' IT COOPs and DRPs are out-of-date, with some as old as 2009. In addition, the Central Office and the facilities are not performing annual tests against the plans.

Criteria

The Security Standard, Section CP-1, requires DBHDS to develop and disseminate procedures to facilitate the implementation of a contingency planning policy and associated contingency planning controls. The Security Standard also requires the agency to maintain current IT COOPs and DRPs and conduct annual tests against the documents to assess their adequacy and effectiveness.

Consequence

By not having current IT COOPs and DRPs, DBHDS increases the risk of mission critical systems being unavailable to support patient services. In addition, by not performing annual tests against the plans, DBHDS is unable to identify weaknesses in the plans and may unnecessarily delay the availability of sensitive systems in the event of a disaster or outage.

Cause

Due to the lack of governance and procedures to ensure consistency, the IT COOPs and DRPs throughout DBHDS are not meeting requirements in the Security Standard, are out-of-date, and are not receiving annual testing.

Recommendation

DBHDS should develop processes and a governance structure to ensure the contingency management program meets the minimum requirements in the Security Standard. DBHDS should develop procedures, assign roles and responsibilities, and update the IT COOPs and DRPs ensuring they are consistent across the agency. DBHDS should also perform annual tests against the plans to ensure Central Office and the facilities can restore mission critical and sensitive systems in a timely manner in the event of an outage or disaster. Doing this will help to ensure DBHDS maintains the confidentiality, integrity, and availability of their mission critical and sensitive systems.

Continue to Upgrade Unsupported Technology
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes

Condition

DBHDS is putting sensitive data at risk by using end-of-life/end-of-support technology for sensitive systems. DBHDS has made progress to upgrade, consolidate, and decommission the end-of-life systems that contain HIPAA data, mission critical financial data, and Personal Health Information (PHI) data. DBHDS made this a priority and hired three external developers and an external business analyst and dedicated internal resources to remediate the end-of-life technology. DBHDS has less than 20 sensitive systems utilizing end-of-life technology and has plans to remediate the remaining end-of-life technology by the end of the first quarter in 2018.

Criteria

The Security Standard, SI-2-COV (c), requires that organizations prohibit the use of products designated as end-of-life/end-of-support by the vendor or publisher.

Consequence

By using end-of-life/end-of-support technology, DBHDS can no longer receive and apply security patches for known vulnerabilities, which increases the risk that a malicious attacker may exploit these vulnerabilities, leading to a data breach. DBHDS has systems using end-of-life technology that contain HIPAA data, and if a data breach occurs, it can result in large monetary penalties, up to $1.5 million. Additionally, vendors do not offer operational and technical support for end-of-life/end-of-support technology, which affects data availability by increasing the difficulty of restoring system functionality if a technical failure occurs.

Cause

DBHDS has a decentralized IT environment and does not maintain a complete inventory of sensitive systems at the Central Office and facilities that includes the software application versions. In addition, DBHDS is not establishing baseline configurations for their sensitive systems. The absence of baseline configurations increases the risk that sensitive systems will not meet the minimum security requirements to protect data from malicious access attempts.

Recommendation

DBHDS should continue to prioritize the upgrade, consolidation, or decommission of all end-of-life/end-of-support technology. In addition, DBHDS should implement mitigating controls for the remaining end-of-life sensitive systems to reduce the risk to the confidentiality, integrity, and availability of sensitive Commonwealth data.

Develop Baseline Configurations for Information Systems
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes

Condition

DBHDS does not have documented baseline configurations for their sensitive systems' hardware and software requirements. DBHDS is working to reduce the total number of sensitive systems, but still has over 200 sensitive systems, with some containing HIPAA data, social security numbers, and Personal Health Information (PHI) data. DBHDS is in the process of implementing software that has the ability to establish, configure, and monitor baseline configurations. DBHDS is working with the Virginia Information Technologies Agency and Northrop Grumman Partnership (Partnership) to install the infrastructure.

Criteria

The Security Standard, Sections CM-2 and CM-2-COV, requires DBHDS to perform the following:

- Develop, document, and maintain a current baseline configuration for information systems;
  (Section 8 Configuration Management: CM-2)

- Review and update the baseline configurations on an annual basis, when required due to environmental changes, and during information system component installations and upgrades;
  (Section 8 Configuration Management: CM-2)

- Maintain a baseline configuration for information system development and test environments that is managed separately from the operational baseline configuration;
  (Section 8 Configuration Management: CM-2)

- Apply more restrictive security configurations for sensitive systems, specifically systems containing HIPAA data; and
  (Section 8 Configuration Management: CM-2-COV)

- Modify individual IT system configurations or baseline security configuration standards, as appropriate, to improve their effectiveness based on the results of vulnerability scanning.
  (Section 8 Configuration Management: CM-2-COV)

Consequence

DBHDS has over 200 sensitive systems, with some containing HIPAA data, social security numbers, and PHI data. The absence of baseline configurations increases the risk that these systems will not meet the minimum security requirements to protect data from malicious access attempts. Baseline security configurations are essential controls in information technology environments to ensure that systems have appropriate configurations and serve as a basis for implementing or changing existing information systems. If a data breach occurs to a system containing HIPAA data, the agency can incur large penalties, up to $1.5 million.

Cause

DBHDS purchased software to assist the agency with documenting and managing baseline configurations. The agency is working with their service provider to install the software in their environment, but this is not complete due to other priorities at the agency.

Recommendation

DBHDS should complete the installation of the software and dedicate the necessary resources to establish and maintain security baseline configurations for their sensitive information systems to meet the requirements in the Security Standard. Doing this will help ensure the confidentiality, integrity, and availability of the agency's sensitive data.

Increase Oversight over Third-Party Providers

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Condition

DBHDS is not gaining annual assurance that their third-party providers have secure IT environments to protect sensitive Commonwealth data. Third-party providers are organizations that perform outsourced business tasks or functions on behalf of the Commonwealth. DBHDS uses a third-party provider for two of its mission critical business functions including its electronic health records system, which contains Commonwealth and HIPAA data relating to patients served by DBHDS, and its waiver management system that supports citizens seeking waivers for individuals with intellectual and developmental disabilities.

Criteria

The Commonwealth's Hosted Environment Information Security Standard, SEC525 (Hosted Environment Security Standard), section SA-9-COV 3.1, requires agencies to perform an annual security audit of the environment or review the annual audit report of the environment conducted by an independent, third-party audit firm on an annual basis.

Consequence

By not gaining assurance over third-party service providers' IT environments, DBHDS cannot validate that they provide effective IT controls to protect its sensitive data.

Cause

DBHDS does not gain assurance over their third-party providers' IT environments because there is no formal process in their information security program for identifying third-party service providers. Thus, there is no expectation to provide the appropriate oversight.

Recommendation

DBHDS should develop a formal process to gain assurance that their third party providers have secure IT environments to protect sensitive data. One way to do this is by requesting and reviewing

Service Organization Controls reports or by review of other independent audit reports as accepted by the Commonwealth's IT Security Audit Standard, SEC502-02.2. After DBHDS develops a formal process, they should incorporate it into their information security program.

Why the APA Audits Capital Assets Management

DBHDS has 15 individual locations throughout the Commonwealth. DBHDS owns over $628 million in capital assets, including the purchase of over $32 million of capital assets during fiscal year 2017. We audit the purchase, management, and reporting of these assets to ensure proper accountability and stewardship. To determine if capital assets are accounted for properly, we compared the practices of DBHDS to those required by the Commonwealth Accounting Policies and Procedures (CAPP) Manual.

Improve Internal Controls over Capital Asset Additions

Type: Internal Control and Compliance
Severity: Deficiency
Repeat: Yes
Prior Title: Improve Policies and Procedures over Fixed Assets

Condition

Individual facilities within DBHDS do not have adequate policies and procedures in place to ensure capital assets are recorded in the Commonwealth's fixed asset system timely. Four out of five facilities recorded 52 percent of their fiscal year 2017 capital asset acquisitions more than 30 days after receipt and acceptance of the asset. In addition, receiving facilities did not properly record 21 out of 24 assets transferred between facilities. These instances include but are not limited to: not recording the transfer of the asset on the receiving facility's books, recording the wrong date of transfer and acquisition, recording the wrong useful life of a transferred asset, and recording the fair value of the asset rather than the current net book value.

Criteria

CAPP Manual Topic 30205 - Acquisition Method states, "All recordable assets, except constructed assets, should be recorded in the Commonwealth's fixed asset system as soon as possible after title passes. Except in unusual circumstances, assets should be posted within 30 days after receipt and acceptance of the asset. Asset acquisitions should be posted to the Commonwealth's fixed asset system in the fiscal year the asset was acquired."

CAPP Manual Topic 30205 - Acquisition Method also states, "Transfers from Other State Agencies - Governmental Accounting Standards Board Statement No. 48, Sales and Pledges of Receivables and Future Revenues and Intra-Entity Transfers of Assets and Future Revenues, requires that an asset transfer between state agencies be treated as a related party transaction. This requires the asset be

recorded at the book value of the transferring entity. The easiest way to accomplish this task is to record the asset at the original historical cost, acquisition date and nomenclature of the disbursing agency."

Consequence

Improper recording of capital assets within the Commonwealth's fixed asset system increases the risk of misstatement of asset balances. These misstatements can ultimately affect DBHDS facility Medicaid reimbursements and the Commonwealth's Comprehensive Annual Financial Report.

Cause

DBHDS does not have adequate processes to ensure timely recording of asset acquisitions in the Commonwealth's fixed asset system or appropriate policies and procedures in place for the recording of transferred assets. DBHDS facilities provided several reasons for delays in asset recording and improper methods of recording transferred assets. These include, but are not limited to: not receiving the Commonwealth's fixed asset system information from the sending facility, not understanding how the asset should be recorded, receiving incorrect Governmental Accounting Standards Board (GASB) guidance from the Internal Audit Director, not having procedures in place to ensure assets are recorded timely, not having a voucher number for the asset purchase to record in the Commonwealth's fixed asset system before the entry deadline, and initially recording the asset under the wrong facility.

Recommendation

Management should create, communicate, and implement policies and procedures over capital asset recording and transfers at all DBHDS facilities and the Central Office. Facilities should handle inspection and processing of facility paperwork promptly enough to ensure recording of assets within 30 days of receipt. Management should ensure personnel involved with capital assets understand the importance of timely asset recording as it affects both depreciation and asset balances. Management should ensure that assets are properly recorded in the Commonwealth's fixed asset system when they are transferred between DBHDS facilities and other state agencies. Internal Audit should ensure that the guidance they provide the facilities follows the most recent GASB pronouncements as well as the CAPP Manual. Management should ensure all documentation used in the process of the transfer is completed and made readily available for the receiving agency or facility at the time of transfer.

Why the APA Audits Financial System Reconciliations

DBHDS has its own financial system and patient billing system where expense and revenue transactions originate and then flow to the Commonwealth's accounting and financial reporting system. Reconciliations between all of these systems is critical to ensure that the financial transactions recorded in the Commonwealth's accounting and financial reporting system accurately reflect the financial operations of the agency. To determine if DBHDS is properly reconciling these systems, we compared the practices of DBHDS to those required by the CAPP Manual.

Improve Internal Controls over Reconciliations

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Condition

Individual facilities within DBHDS do not have adequate controls in place to ensure reconciliations between DBHDS financial systems are performed timely and at the appropriate level, are materially correct, are signed by the preparer, and are properly reviewed. During our review, we found the following:

- One of six facilities tested did not complete a reconciliation between the Commonwealth's fixed asset system, DBHDS' financial system, and the Commonwealth's accounting and financial reporting system. In addition, two facilities did not review their reconciliation between these systems for a month and three months respectively, after preparation, which is untimely.

- Two of six facilities tested are not performing reconciliations at the appropriate level (i.e. fund, program, and account).

- One of six facilities tested did not have the appropriate reviewer signature and completion dates on the reconciliations.

- One of six facilities tested did not have the appropriate preparer signature and completion dates on the reconciliations.

- One of six facilities tested did not include the proper month end balances on their reconciliation between DBHDS' billing system, DBHDS' financial system, and the Commonwealth's accounting and financial reporting system. Month end balances included refunds that should not have been included.

Criteria

CAPP Manual Topic 20905 – Cardinal Reconciliation Requirements requires all internally prepared accounting records, data submission logs, and other accounting data to be reconciled to reports produced by the Commonwealth's accounting and financial reporting system by the last business day of the month following the period close. In addition, Topic 20905 prescribes the level of detail at which agency records, accounts, and logs must be reconciled depending on the nature of the transactions. Finally, by submitting the Certification of Agency Reconciliations to the Department of Accounts (Accounts), the agency is certifying that its internal records will be in agreement with those reported in the state-wide financial system, and that all cash balances, appropriations, allotments, total expenses, net revenues, and fixed assets have been reconciled at the appropriate level.

Consequence

The improper reconciliation of systems to the Commonwealth's accounting and financial reporting system, and the lack thereof, increases the risk of material misstatement of overall account balances. These misstatements can ultimately affect funding for DBHDS services and the amounts DBHDS reports for the Commonwealth's Comprehensive Annual Financial Report.

Cause

DBHDS facilities provided several reasons for the lack of a reconciliation, the improper review of a reconciliation, and the improper completion of a reconciliation. These include, but are not limited to: availability of personnel, not adhering to the facility's policy and procedures over system reconciliation, being unaware that specific reconciliations are needed, being unaware that the preparer should sign the reconciliations, being unable to prepare the reconciliations at the appropriate level because the appropriate reports are not available, and being unaware that reconciliations must be completed at the account level.

Recommendation

Management should reinforce policies and procedures over system reconciliations for DBHDS facilities. Management should ensure that CAPP Manual requirements reflected in policies and procedures are communicated to personnel and adhered to when completing reconciliations. Facilities should be reconciling at the correct level for each system reconciliation. Facilities should ensure that they perform all required reconciliations for all systems used. Management should ensure that the appropriate preparer and reviewer sign each reconciliation step. The facilities should submit monthly certifications to Accounts only after they complete all required reconciliations.

Why the APA Audits an Agency's Controls Over their Information in the Commonwealth's Retirement Benefits System

The Commonwealth's Retirement Benefits system is used to calculate total pension liabilities for the Commonwealth. Individual agencies are responsible for updating the records within the Retirement Benefits system related to their employees. As a result, DBHDS' management must take adequate precautions to ensure the integrity of these records. To determine if management implemented these precautions, we compared the practices of DBHDS to the guidance provided by Accounts and the Virginia Retirement System (VRS).

Improve Controls Over the Commonwealth's Retirement Benefits System

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes

Condition

Individual facilities within DBHDS do not have adequate controls in place to ensure that retirement information for employees is accurate, specifically:

- Four of five (80 percent) facilities tested did not clear exceptions identified on the Commonwealth's payroll system automated reconciliation reports timely.

- Two of five (40 percent) facilities tested did not maintain documentation showing that they review the Commonwealth's human resource system cancelled records reports regularly and clear exceptions noted on the report.

- Four of eight (50 percent) facilities tested did not perform reconciliations of creditable compensation between the Commonwealth's retirement benefits system and human resource system. As a result, these facilities also did not perform a complete reconciliation prior to certifying the retirement benefits system snapshot.

- Three of five (60 percent) facilities tested did not clear reconciling items on the creditable compensation reconciliation prior to certifying the snapshot.

- One of eight (13 percent) facilities tested did not have policies and procedures for performing the creditable compensation reconciliation between the Commonwealth's retirement benefits system and human resource system.

- Two of fifteen (13 percent) terminated retirement benefits system users tested did not have their access removed timely (within three business days). Removal for these users took between four and 11 days.

Criteria

Accounts Payroll Bulletin Volume 2013-02 states that agencies should review transactions appearing on the Commonwealth's human resource system cancelled records report and correct those items prior to certifying the monthly contributions snapshot. Additionally, the Payroll Bulletin states that agencies should review the Accounts automated reconciliation reports after the monthly snapshot and make corrections for those items appearing on the reports. CAPP Manual Topic 50410 – Retirement – VRS and Optional Retirement Plans (ORP) states that agencies should reconcile creditable compensation between the Commonwealth's human resource system and retirement benefits system monthly prior to certifying the snapshot. Lastly, facility-specific policies and procedures require removal of retirement benefits system access within three business days of user termination or reassignment.

Consequence

Improper pre and post certification processes can affect the integrity of the information in the Commonwealth's retirement benefits system that determines pension liability calculations for the entire Commonwealth. Delays in deleting access increases the risk of unauthorized use of the retirement benefits system by terminated employees, which could result in unauthorized changes and could impair data integrity. Since the VRS actuary uses the retirement benefits system data to calculate the Commonwealth's pension liabilities, inaccurate data could result in a misstatement in the Commonwealth's financial statements.

Cause

Staffing shortages, turnover, and a lack of understanding of pre and post certification procedures contributed to the deficiencies noted above.

Recommendation

Management should ensure adequate policies and procedures for the Commonwealth's retirement benefits system exist to guide facility staff performing monthly retirement benefits system reconciliations and should implement additional policies and procedures where necessary. Additionally, facility staff should clear exceptions noted in the Commonwealth's human resource system cancelled records report and the Commonwealth's payroll system automated reconciliation reports timely. When clearing exceptions, facility staff should document the reason for the exception and the remediation activities performed. Management should remove access for terminated employees with access to the Commonwealth's retirement benefits system within three business days.

Why the APA Works with DBHDS Internal Audit to Audit Payroll

DBHDS employs over 10,000 salaried and wage employees across 15 facilities. Because of the sizeable nature of this expense to the Commonwealth, DBHDS management must take necessary precautions to ensure the integrity of payments to employees. To determine if controls over payroll were adequate, DBHDS Internal Audit compared the practices of DBHDS to those required by the CAPP Manual.

Improve Controls over Payroll

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Condition

Individual facilities within DBHDS do not have adequate controls in place to ensure human resources forms are completed, payroll is appropriate, and access is removed timely. Specifically:

- Five out of 47 (11 percent) DBHDS' attendance and leave system users tested did not have a properly signed and approved access form; 12 out of 47 (26 percent) DBHDS' attendance and leave system users tested had an access level provided by the facility that did not match their approved access form; and one out of 47 (two percent) DBHDS' attendance and leave system users tested separated on October 29, 2016, but their access was not deleted for over eight months.

- Three out of 73 (four percent) Commonwealth's payroll system users tested did not have their access deleted for five to nine weeks after separation from DBHDS.

- Four out of 35 (11 percent) Commonwealth's human resource system users tested did not have their access timely deleted. Two of the four users had access for four and 20 weeks after separation, and the other two users had access for an undeterminable length of time after separation because there was no documentation of when DBHDS deleted access.

- Two out of 16 (13 percent) Commonwealth's human resource system exception reports tested did not have proper documentation of issues on the report being resolved and 12 out of 16 (75 percent) resolved exception report issues tested were not properly reviewed and approved.

- Eight out of 120 employees (seven percent) tested in regular payroll had instances where the Payroll department did not receive authorizing documentation containing any management signatures outside of the Human Resources department for all types of changes in pay.

- Thirty-six out of 84 (43 percent) separated employees tested either did not have a clearance checklist within their personnel file or the checklist did not have the appropriate signatures, one out of 84 (one percent) separated employees tested had a personnel action form that was not received or processed by the Payroll department, and one out of 84 (one percent) employees tested was not removed from the Commonwealth's payroll system for over 20 weeks after separation.

Criteria

CAPP Manual Topic 50505 - Time and Attendance states that agencies must verify that all source documents such as timecards, timesheets, or any other authorization used to pay or adjust an employee's pay have been properly completed, authorized by the appropriate party, and entered accurately into the Commonwealth's payroll system.

The Security Standard, Section AC-2-COV 2 e and f, requires the prompt removal of system access for terminated or transferred employees. The Security Standard, Section AC-2-COV 2 a, requires granting access to the system based on a valid access authorization. The Security Standard, Section AC-6, requires agencies to employ the principle of least privilege allowing only authorized access for users, which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Consequence

Not having proper approval of payroll forms and pay changes increases the risk that DBHDS could pay unauthorized and incorrect salaries. Not properly removing access of terminated and resigned employees increases the risk of unauthorized individuals inappropriately entering or approving transactions and could compromise sensitive employee information. Not having proper review of the Commonwealth's payroll system to the Commonwealth's human resource system exception reports and approval of changes made to clear exceptions could result in erroneous payments being made or payments that exceed classification limits.

Cause

These exceptions occurred because the individual facilities either do not have adequate policies and procedures for payroll forms or did not comply with established CAPP Manual guidance or local policies and procedures for payroll forms. Additionally, the exceptions resulted from a lack of communication and understanding between the Human Resources and Payroll departments.

Recommendation

Management across all DBHDS facilities, not just those tested, should evaluate and update policies and procedures to provide adequate guidance to ensure proper approval and completion of employee work profiles, payroll forms, and pay changes. In addition, Human Resource and Payroll

personnel, across all facilities, should ensure that they receive properly approved and completed employee work profiles, payroll forms, and pay changes before processing these changes. Lastly, management for all facilities should remove all access for employees that terminated, resigned, or no longer needed access timely.

Department of Health

Why the APA Audits Information System Security

Health collects, manages, and stores significant volumes of personal and financial data within its mission critical systems. Because of the highly sensitive and critical nature of this data, Health's management must take all necessary precautions to ensure the integrity and security of the data in its systems. We compared Health's practices to those required by the Commonwealth's Information Security Standard in the areas of web application security, oversight of sensitive systems, and information system access.

Improve Timely Removal of Critical Access

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes

Condition

Individual department supervisors are not completing and sending employee separation forms (HR-14) to the Office of Human Resources (OHR) timely. As a result, Health does not remove information system access for terminated employees promptly as shown in the following instances:

- Local Health Department (LHD) system access was removed eight to 131 days late for six out of 24 (25 percent) employees;
- Payroll system access was removed six to 40 days late for ten out of 17 (59 percent) employees;
- Benefits system access was removed four to 42 days late for eight out of 15 (53 percent) employees; and
- Network access was removed five to 14 days late for three out of 25 (12 percent) employees.

Criteria

The Security Standard, Section 09.1 AC-2 (h), requires, "Notifying account managers…when information system users are terminated, transferred, or information system usage or need-to-know changes." In addition, Security Standard, Section 09.1 AC-2-COV (2.f), states that each agency shall "promptly remove access when no longer required."

Health internal policies also state the HR-14 should be processed within three business days of receipt by OHR.

Consequence

Terminated employees who still have network access may be able to access other critical programs since it acts as the gateway to all the agency's systems. Untimely removal of LHD access increases the risk that employees could use their inappropriate access to gather sensitive patient information. Untimely removal of access to payroll and benefits systems increases the risk that employees could use their inappropriate access to make changes to payroll related items.

Cause

There are a number of different problems contributing to this issue. First, individual department supervisors are not completing and sending the HR-14 to OHR as required by Health's policy. When an employee terminates it is the responsibility of the work unit to notify OHR of the departure. Due to the decentralized nature of Health, this does not always happen timely. Additionally, the HR-14 is not being routed to and signed off by individual areas such as the Office of Information Management, Office of Finance Management, and others for their input as to critical system access. Lastly, OHR is not properly completing or processing the HR-14.

The following specific instances contributed to the untimely removal of system access for terminated employees:

- Individual departments did not properly complete the HR-14 for 16 of 25 (64 percent) terminated employees;
- Individual work units did not submit the HR-14 timely to OHR for 15 of 25 (60 percent) terminated employees;
- OHR did not properly complete the HR-14 for 21 of 25 (84 percent) terminated employees;
- OHR did not process the HR-14 timely for eight of 25 (32 percent) terminated employees; and
- OHR did not document the critical access removal date on the HR-14 for seven of 25 employees (28 percent).

Recommendation

We previously reported that Health had made improvements in the HR-14 process; however, our work this year shows that the process is not working effectively and Health needs to continue to focus on this area. Health management should consider a thorough review of OHR operations due to their critical role in the HR-14 process given that problems in this process seem to be an underlying cause for many of the untimely access removals. In addition, the process surrounding completion and routing of the HR-14 should be reviewed and updated to ensure that system access is removed timely.

Improve Database Security
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Condition

Health does not secure a sensitive system's supporting database with some minimum security controls. We communicated the control weaknesses to management in a separate document marked Freedom of Information Act (FOIA) Exempt under §2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

Criteria

The Security Standard requires the implementation of certain controls that reduce unnecessary risk to data confidentiality, integrity, and availability in systems processing or storing sensitive information.

Consequence

By not meeting the minimum requirements in the Security Standard and aligning the database's settings and configurations with best practices, Health cannot ensure the confidentiality, integrity, and availability of data within the database.

Cause

Health's security baseline configuration does not align settings and configurations with Security Standard requirements and best practices.

Recommendation

Health should dedicate the necessary resources to evaluate and implement the controls discussed in the communication marked FOIA Exempt in accordance with the Security Standard in a timely manner.

Why the APA Audits the Child and Adult Care and Feeding Program (CACFP)

The CACFP program provides approximately $52 million annually to initiate and maintain non-profit food service programs for eligible children and adults in nonresidential day care settings. The program consists of nutritious meals and snacks served to eligible children and adults who are enrolled for care at participating childcare centers, adult day care centers, outside-school-hours care centers, at-risk afterschool programs, family and group day care homes, and emergency shelters. We reviewed time and effort reporting, allowable costs, procurement, reporting, and sub-recipient monitoring.

Strengthen Subrecipient Monitoring Process
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Condition

The Office of Family Health Services, Special Nutrition Programs (SNP) is not completing new sponsor reviews as required for the CACFP program. SNP did not perform the required review for one of four (25 percent) newly added sponsors, with five or more sites, within the first 90 days of operation. The review is over 250 days late.

Criteria

Code of Federal Regulations (CFR) 7 CFR §226.6 (6) (iii) requires new sponsoring organizations of five or more facilities to be reviewed within the first 90 days of program operations.

Consequence

Failure to review new sponsors within 90 days could result in questioned costs and possible loss of funding.

Cause

SNP does not have documented procedures for the review schedule for new sponsors. In addition, the process for determining reviews is manual, leading to missed or overlooked scheduling for sponsor reviews.

Recommendation

SNP should ensure that their subrecipient monitoring procedures are documented and kept current. SNP should also work to develop an electronic process for identifying new sponsors and determining if they have five or more sites.

Why the APA Audits Access Management for the Claims Processing System

The current claims processing system (current system) is accessible from the web; stores protected health information for over one million individuals; and is used to process over $9 billion in medical claims annually. While the current system is operated by a contractor, the Department of Medical Assistance Services (Medical Assistance Services) is the system owner and is responsible for ensuring that the current system is managed in accordance with the Commonwealth's Information Security Standard, SEC501-09 (Security Standard). To evaluate Medical Assistance Services' management of access for the current system, we compared internal control practices to those required by the Security Standard. Collectively, the following four findings and recommendations, three related to the current system and another one related to performing an information technology review, represent a material weakness.

Develop Processes to Facilitate the Controlling of Privileges in the Claims Processing System

Type: Internal Control and Compliance
Severity: Material Weakness
Repeat: No

Condition

Medical Assistance Services' Office of Compliance and Security (Compliance and Security) completed a conflict matrix documenting certain combinations of privileges that create internal control weaknesses in its current system. However, the conflict matrix does not document all combinations of over 900 capabilities within the current system that may create internal control weaknesses.

Criteria

The Security Standard, Section 8.1 AC-1, requires agencies to develop, document, and disseminate formal documented procedures to facilitate the implementation of the access control policy and associated access controls. The access control policy and procedure should also be reviewed and updated on an annual basis or more frequently if required to address an environmental change. Additionally, Section 8.1 AC-2(c) and (d) requires that agencies establish conditions for group membership and specify access privileges.

Consequence

Without complete documentation of conflicting privileges in the current system and providing it to the managers responsible for reviewing system access, management is increasing the risk of granting

employees capabilities that violate the concept of segregation of duties or the principle of least privilege, thereby creating an internal control weakness.

Cause

According to management, the current system is a 14-year-old, highly complex system that lacks the reporting features and automated review processes necessary to effectively and efficiently manage system access and security. Medical Assistance Services' prior year corrective action plan for the finding titled "Create Formal Documentation that Facilitates Controlling Privileges…" states the agency would develop a conflict matrix for use with a manual access review process in order to mitigate the risks associated with the current system. However, according to management, the agency would have to acquire additional resources in order to completely and accurately document all capabilities and potential conflicts within the current system. Consequently, management determined it would avoid using resources on a system that will be replaced in 2018 with a new claims processing system (new system).

Recommendation

Medical Assistance Services should continue to perform manual access reviews and review for violations of the concept of segregation of duties and the principle of least privilege within the current system. In addition, Compliance and Security should gain an understanding of the security environment in the new system and ensure it establishes a process to document and evaluate system access by completing a conflict matrix and incorporating the documentation into the annual access evaluation process.

Remove Access to the Current Claims Processing System in a Timely Manner
Type: Internal Control and Compliance
Severity: Material Weakness
Repeat: No

Condition

Medical Assistance Services did not remove access to the current system for individuals who no longer needed access. Specifically, eight of 16 of the separated employees listed on the access report did not have their access suspended within 24 business hours. The eight employees in question retained their unsuspended access between seven and 34 days after separation.

Criteria

Per Medical Assistance Services' IT Access Control AC-1 Policy Section A11(b)(i), "All user accounts must be disabled immediately upon separation or within 24 business hours upon receipt by the Office of Compliance and Security." In addition, Security Standard, Section 8.13, states an organization must disable information system access within 24 hours of employee separation and terminate any authenticators or credentials associated with the individual.

Consequence

Not suspending access to a web based mission critical system that can be accessed from anywhere in the world after employee separations threatens the data integrity of the system. If separated employees retain access to the current system, users are potentially able to view, copy, and edit sensitive information.

Cause

Compliance and Security is not suspending separated employees' access in a timely manner due to ineffective and untimely communication with Medical Assistance Services' Human Resources Division.

Recommendation

Compliance and Security and the Human Resources Division should establish effective, regular communication to report staff changes to those individuals responsible for managing system access. In addition, Compliance and Security should ensure compliance with its Access Control Policy and the Security Standard by removing users' access as required.

Complete Annual Review for the Current Claims Processing System

Type: Internal Control and Compliance
Severity: Material Weakness
Repeat: No

Condition

Medical Assistance Services' Compliance and Security did not complete an annual access review for one of the three user groups of the current system. Compliance and Security completed an annual access review of the Virginia Department of Social Services (Social Services) and contractors' user groups; however, it did not perform an annual review of Medical Assistance Services employees. The most recent review of Medical Assistance Services employees' system access was completed in April 2016. As of August 1, 2017, Compliance and Security had not started its review of Medical Assistance Services employees.

Criteria

The Security Standard, Section 8.1, requires the agency to "review accounts for compliance with account management requirements on an annual basis or more frequently if required to address an environmental change."

Consequence

Not conducting regular reviews of users' access to mission critical systems threatens the integrity of the system and the data housed within the system. If Medical Assistance Services employees retain access to unnecessary capabilities in the current system, the risk of improper segregation of duties increases. As a result, the risk of unreliable or incorrect information also increases.

Cause

According to management, Compliance and Security understood the Security Standard criteria noted above to mean once every calendar year. Therefore, Compliance and Security did not perform its review of Medical Assistance Services employees' access during fiscal year 2017.

Recommendation

Compliance and Security should perform an annual review of its employees' access to the current system in order to identify unnecessary access due to terminations or changes in job responsibilities. In addition, Compliance and Security should ensure compliance with the Security Standard and ensure its policy identifies the specific time in which the annual review should occur.

Why the APA Audits Security Compliance Audits

Medical Assistance Services uses a number of information systems to administer the Medicaid program. Many of these systems contain sensitive, protected health and/or financial information. While some of the systems used to administer the program are operated by a contractor, Medical Assistance Services is still required to implement policies, procedures, and processes that meet the requirements of the Security Standard and Health Insurance Portability and Accountability Act (HIPAA). The federal government requires management at Medical Assistance Services to monitor their compliance with these security requirements. We evaluate the results of these audits to ensure issues are addressed and corrective action plans are followed. Collectively, the preceding three findings and recommendations related to the current system and the following finding and recommendation related to performing an information technology review represent a material weakness.

Perform the Required Information Technology Review
Type: Internal Control and Compliance
Severity: Material Weakness
Repeat: Yes
Prior Title: Perform Information Technology Review as Required

Condition

Since January 31, 2014, Medical Assistance Services has not completed the required biennial Automated Data Processing (ADP) risk analyses and system security review. In January 2017, Medical Assistance Services' Internal Audit Division contracted with an external service provider to perform the required security review of the current system. However, the review has not been finalized, and Medical Assistance Services has not received a final report from the external service provider as of October 2017.

Criteria

As required by 42 CFR §95.621, Medical Assistance Services must review on a biennial basis its current system security program. At a minimum, the review shall include an evaluation of physical and data security operating procedures and personnel practices. In addition, 42 CFR §95.621(f)(1) requires state agencies to determine the appropriate ADP security requirements based on recognized industry standards or standards governing security of federal ADP systems and information processing.

The Security Standard, Section 1.1, states that agency heads remain accountable for maintaining compliance with the Security Standard for IT equipment, systems, and services procured from providers and must enforce the compliance requirements through documented agreements and oversight of the services provided.

Consequence

Without the biennial review, Medical Assistance Services cannot ensure that controls over its current system, maintained by the provider, are designed, implemented, and operating effectively. Although Medical Assistance Services maintains a high degree of interactions with its provider, it is increasing the Commonwealth's risk that it will not detect a weakness in the provider's environment, which could negatively impact the Commonwealth. Due to the highly sensitive, mission critical nature of the data and controls within the current system, Medical Assistance Services is also compromising system integrity and increasing the risk of unauthorized system access. Additionally, because the U.S. Office of Management and Budget included the requirement for ADP risk analyses and system security review in its Compliance Supplement, this issue will result in the Medicaid Program receiving a qualified opinion on compliance.

Cause

According to management, Medical Assistance Services incorrectly assumed that the results of a review conducted by the U.S. Department of Health and Human Services during fiscal year 2016 could be used to meet both federal and state requirements for Medical Assistance Services to conduct an information technology review. However, management was not able to obtain an assertion from the federal government that its review would satisfy Medical Assistance Services' responsibility.

Recommendation

Medical Assistance Services should ensure that the required biennial review is completed and that future reviews are completed and are arranged to meet the timing and other requirements. In addition, Medical Assistance Services should use the results of these reviews to ensure its provider complies with the requirements in the Security Standard, Commonwealth Accounting Policies and Procedures (CAPP) Manual, Code of Federal Regulation, and contract with the Commonwealth. If weaknesses are disclosed from the required review, Medical Assistance Services should implement complementary controls to mitigate the risk to the Commonwealth until the provider corrects the deficiency.

Why the APA Audits Management's Use of Third Party Service Provider Audit Reports

Medical Assistance Services uses several third party service providers to facilitate the collection and storage of financial and sensitive, protected health information that is material to the Commonwealth's financial statements and federal programs. While these services are not directly performed by Medical Assistance Services, Medical Assistance Services must maintain oversight and ensure that the internal control environment established by the third party service providers is consistent with the services in the contract as well as the Security Standard. To ensure that Medical Assistance Services is properly monitoring third party service providers, we evaluated whether management was properly obtaining, reviewing, and reacting to their service provider audit reports.

Review and Document Service Organization Control Reports of Third-Party Service Providers

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes

Condition

Medical Assistance Services does not review each of its third-party service providers' (providers) Service Organization Control reports. Providers are entities that perform outsourced tasks and business functions on behalf of Medical Assistance Services and the Commonwealth. A Service Organization Control report provides an independent description and evaluation of the provider's internal controls. Although Medical Assistance Services works closely with its providers, management should regularly review Service Organization Control reports and document the results of its reviews in order to ensure the effectiveness of providers' controls.

Criteria

The Security Standard, Section 1.1, states that agency heads remain accountable for maintaining compliance with the Security Standard for information technology equipment, systems, and services procured from providers, and agencies must enforce the compliance requirements through documented

agreements and oversight of the services provided. Additionally, the CAPP Manual Topic 10305 requires agencies to have adequate interaction with the provider to appropriately understand the provider's internal control environment. Agencies must also maintain oversight over the provider to gain assurance over outsourced operations.

Consequence

Without performing a review of Service Organization Control reports, Medical Assistance Services cannot ensure that providers' controls are designed, implemented, and operating effectively. Although Medical Assistance Services maintains a high degree of interactions with its providers, management is increasing the Commonwealth's risk that it will not detect a weakness in a provider's environment, which could negatively impact the Commonwealth.

Cause

According to management's corrective action plan dated September 30, 2017, Medical Assistance Services is still developing its process, policies, and procedures for reviewing, assessing, and documenting the results of the Service Organization Control reports as a method to evaluate provider controls. In addition, management is still working to determine which Medical Assistance Services employees should be responsible for reviewing the reports.

Recommendation

Medical Assistance Services should develop and implement policies and procedures to review, assess, and document the effectiveness of provider controls reported through Service Organization Control reports. In addition, Medical Assistance Services should use Service Organization Control reports as a component of its oversight activities over its providers to confirm they comply with the requirements outlined in the Security Standard, CAPP Manual, and industry best practices. If weaknesses are identified in Service Organization Control reports, Medical Assistance Services should implement complementary controls to mitigate the risk to the Commonwealth until the provider corrects the deficiency.

Why the APA Audits Access Management for the Commonwealth's Procurement System

In fiscal year 2017, Medical Assistance Services used the Commonwealth's procurement system to procure over $100 million in goods and services. While the Department of General Services administers the Commonwealth's procurement system, Medical Assistance Services uses the system to control the procurement process between the requisitioner and supplier. As a result, Medical Assistance Services is responsible for ensuring proper access to the procurement system. To evaluate Medical Assistance Services' management of access, we compared its internal practices to the Security Standard applicable to the procurement system.

Ensure Employees have Proper Access Roles within the Commonwealth's Procurement System

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Condition

Medical Assistance Services is not effective in ensuring that employees have proper access roles within the Commonwealth's procurement system. For the entire fiscal year 2017, Compliance and Security did not remove the previous Interim Director of the Procurement and Contract Management Division's "No Supervisor" role in the procurement system. Additionally, during this same time, the current Director of the Procurement and Contract Management Division did not have the "No Supervisor" role in the procurement system. Users with the "No Supervisor" role may retrieve all requisitions for all employees in their chain of direct reporting in the procurement system.

Criteria

Section 5.1 of the procurement system's Security Standard requires that the System Security Officer monitor system access and permissions. In addition, Section 5.2 requires that the System Security Officer perform quarterly access reviews to determine if changes in users' job duties are appropriately reflected in system access and to determine if users who no longer require system access have been removed.

Consequence

Compliance with the procurement system's Security Standards referenced above is necessary to prevent employees from potentially making unauthorized purchases or approvals. Additionally, it is important for the Director of the Procurement and Contract Management Division to have the "No Supervisor" role within the procurement system. Without this role, they are unable to properly monitor the requisitions of all employees in their chain of direct reporting.

Cause

Compliance and Security fulfills the role of the System Security Officer for Medical Assistance Services and as a result is responsible for completing the required quarterly access reviews. However, Compliance and Security did not collaborate with the business process owner, the Procurement and Contract Management Division, to determine the appropriateness of users' access. Although Compliance and Security performed system access reviews during fiscal year 2017, it did not identify that an employee who had previously served as the Interim Director of the Procurement and Contract Management Division was improperly retaining the "No Supervisor" role within the procurement system.

Recommendation

Medical Assistance Services should ensure that employees only have access levels appropriate for them to perform their assigned job duties. In addition, Medical Assistance Services should utilize the assigned "Entity Lead" within the Procurement and Contract Management Division to communicate any necessary changes in access to the System Security Officer. The Entity Lead is an individual whose responsibilities would include working with the System Security Officer and the Department of General Services to ensure proper user access is established and maintained. This liaison between the procurement function and the System Security Officer would contribute to an environment where necessary changes to access are being regularly disseminated to the System Security Officer so they can be effective in ensuring that employees have proper access roles within the procurement system.

Why the APA Audits Transmission of Sensitive Information

As part of administering medical assistance programs, Medical Assistance Services manages, stores, and communicates significant volumes of sensitive data with other state agencies. Due to the highly sensitive and critical nature of this data, Medical Assistance Services must take the necessary precautions to ensure the data is not vulnerable to interception by unauthorized parties when communicating with other state agencies. To evaluate the transmission of sensitive information, we compared Medical Assistance Services' practices and internal policies and procedures to the Security Standard.

Correct Policies and Procedures for E-mailing Sensitive Information to State Agencies
Type: Internal Control and Compliance
Severity: Deficiency
Repeat: No

Condition

Medical Assistance Services incorrectly instructed its employees that they did not have to use a data protection mechanism, encryption, when e-mailing sensitive information to another state agency. As a result, Medical Assistance Services' employees exchanged sensitive information within the agency and to other state agencies through unsecured, unencrypted e-mail.

Criteria

The Security Standard, Section SC-8-COV, requires the use of data protection mechanisms for the transmission of e-mails and attached data that are sensitive. Sensitive data includes, but is not limited to, personally identifiable information. The Commonwealth defines personally identifiable information as information that describes, locates, or indexes anything about an individual such as financial transactions, Social Security Numbers, medical history, ancestry, religion, political ideology, criminal or employment records, and photographs.

Consequence

When Medical Assistance Services' employees do not utilize e-mail encryption or another appropriate method of transmitting sensitive data, the data is vulnerable to interception by unauthorized parties. This increases the risk of unauthorized release of sensitive information about Medicaid recipients, which could expose them to fraud or identity theft.

Cause

Medical Assistance Services' policies and procedures state "E-mail containing PHI sent to state agencies whose e-mail address ends in 'Virginia.gov' (ex. @dss.virginia.gov) will automatically be encrypted, thus no 'Encrypt Message' is needed." The Commonwealth's e-mail system is neither encrypted nor immune to breaches by unauthorized parties. According to management, upon the Virginia Information Technologies Agency's transformation, Medical Assistance Services' Compliance and Security requested confirmation that the Commonwealth's e-mail system is inherently secure. No such confirmation was received. Compliance and Security did not pursue further confirmation, and developed policies and procedures that reflected this incorrect assumption.

Recommendation

Medical Assistance Services should develop and implement policies and procedures for its employees to transmit personally identifiable information securely and in accordance with the Security Standard. Medical Assistance Services should ensure that all employees understand their responsibility and monitor for compliance.

Why the APA Audits the Social Security Number Verification Process

The Social Security Verification Process ensures recipients are eligible for the services provided by the Medicaid Program and the Children's Health Insurance Program. If Medical Assistance Services is not able to resolve Social Security Number discrepancies in a timely manner, medical services may be provided to ineligible individuals. To evaluate the Social Security Number Verification Process, we reviewed Medical Assistance Services' process and reports used to identify outstanding Social Security Number discrepancies for recipients.

Develop Procedures and Performance Expectations for Resolving Social Security Number Discrepancies

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Condition

As of August 2017, the number of Medicaid recipients with Social Security Number (SSN) discrepancies that remain uncorrected after 12 months is 523. While this is an increase of 316 from the prior August, with just over one million individuals receiving Medicaid services, the 523 discrepancies represent one-twentieth of a percent of the total Medicaid population for Virginia. Monthly, Medical Assistance Services provides the Department of Social Services (Social Services) with all SSN discrepancies on the Social Security Number and Citizenship Report (RS-O-485A report) that require resolution.

Criteria

As required by 42 CFR 435.910(g), "The agency must verify each SSN of each applicant and recipient with the SSA [Social Security Administration], as prescribed by the Commissioner, to ensure that each SSN was furnished to that individual, and to determine whether any others were issued." In addition, 42 CFR 435.920 states, "In redetermining eligibility, the agency must review case records to determine whether they contain the recipient's SSN or, in the case of families, each family member's SSN."

Consequence

Medical Assistance Services relies on Social Services to determine individuals' Medicaid eligibility, and Social Services uses SSNs to identify and enroll recipients. This process ensures recipients are eligible for the services provided. If Medical Assistance Services and Social Services are not able to resolve SSN discrepancies in a timely manner, ineligible individuals could receive Medicaid services.

Cause

Medical Assistance Services did not provide Social Services with the entire RS-O-485A report for the first three months of fiscal year 2017. Additionally, Medical Assistance Services has not created, implemented, and maintained policies and procedures for the SSN verification process. Finally, Medical Assistance Services has not developed a baseline performance expectation for Social Services to achieve, given that in the case of newborns, Medical Assistance Services will not deny services after their first birthday if a SSN is not provided.

Recommendation

Medical Assistance Services should provide Social Services with the RS-O-485A report every month. Additionally, Medical Assistance Services should create, implement, and maintain policies and procedures for the SSN verification process. Finally, Medical Assistance Services should develop baseline performance expectations for Social Services related to resolving SSNs. Management of both Medical Assistance Services and Social Services should monitor performance and make adjustments, as needed, to meet expectations.

Why the APA Audits the Annual Accrual Process

Medical Assistance Services' medical claims payable and related federal receivable accrued at year-end are material to the Commonwealth's Comprehensive Annual Financial Report (CAFR). As a result, it is important for Medical Assistance Services to have a thorough understanding of how the accrual methodology, which uses projected and actual data, impacts the financial information it provides to the Department of Accounts (Accounts) for inclusion in the CAFR. To evaluate Medical Assistance Services' claims payable and related federal receivable, we reviewed Medical Assistance Services' accrual methodology and asked for explanations when certain claims data was more than three standard deviations outside of historical trends.

Improve Collective Knowledge of Annual Accrual Reporting

Type: Internal Control
Severity: Material Weakness
Repeat: No

Condition

Medical Assistance Services' Budget Division did not sufficiently explain why its Fiscal Division reported a one percent decrease in accrued claims as of fiscal year-end 2017, which is inconsistent with historical trends and the Budget Division's forecast for a ten percent increase in total claims expenses for fiscal year 2018. Portions of fiscal year 2018 expenses settle claims from fiscal year 2017.

Criteria

Financial report preparation and the components therein, as a best practice, should follow sufficient policies and procedures to prevent and detect potential errors or omissions. As a best practice, collectively, both the Fiscal and Budget Divisions should understand the accrual methodology used to estimate financial information reported to Accounts for the Commonwealth's CAFR.

Consequence

The Fiscal Division reported a one percent decrease in accrued claims from the prior year; however, the Budget Division forecasted of a ten percent increase in expenses without seeking an explanation, which enhances the risk that there could potentially be an undetected error in one of their amounts. Without adequately understanding how projected and actual data impacts the financial information reported to Accounts, management cannot ensure the accuracy of its financial condition. Additionally, incomplete policies and procedures increase the risk that Medical Assistance Services records and reports inaccurate information for inclusion in the CAFR.

Cause

The employees responsible for determining the claims payable and related federal receivable accrual process have changed multiple times during the last three fiscal years. Additionally, the Budget Division does not have complete policies and procedures that document the accrual process or provide guidance for oversight. Finally, the Fiscal Division did not question the estimate when the actual accrual amount for July and August 2017 was $76 million less than what was originally estimated and the estimation for later months was not adjusted.

Recommendation

Medical Assistance Services should ensure that, collectively, its Divisions have a sufficient understanding of the claims payable and related federal receivable accrual process. In addition, the Budget Division should actively collaborate with the Fiscal Division in order to provide the most accurate information to Accounts. Medical Assistance Services should create, implement, and maintain formal policies and procedures that provide sufficient direction for personnel to prepare the accrual schedules and to know when to question items that are outside of expected results and/or are not consistent with historical trends.

Why the APA Audits Collection Efforts

Medical Assistance Services has several utilization units (units) that have the combined responsibility to identify suspected fraud, waste, and/or abuse across the Medicaid Program. In cases where the units find that funds are to be returned, Medical Assistance Services has a set of procedures it is to follow to increase the likelihood that funds are returned. To evaluate collection efforts, in cases where the units determined that funds needed to be returned, we compared Medical Assistance Services' actions to its internal policies and procedures.

Improve the Accounts Receivable Collection Process

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes
Prior Title: Continue Improving Accounts Receivable Collection Process

Condition

In certain cases, Medical Assistance Services' Fiscal Division did not pursue collections from providers and recipients timely and in accordance with its policies and procedures. In certain cases tested from the Program Integrity Units, Medical Assistance Services' actions have resulted in a delay of possible collections. Specifically for each, we found:

- Of the Provider Review Unit cases we tested, seven identified overpayments. In each of these cases, or 100 percent, follow-up collection procedures were not followed.

- Of the Recipient Audit Unit cases we tested, 16 identified overpayments, 11 of which management determined collectable; however, in eight cases, or 73 percent, follow-up collection procedures were not followed.

- Of the Prior Authorization and Utilization Review (PAUR) mental health provider cases we tested, six identified overpayments, three of which management determined collectable; however, in one case, or 33 percent, management was not able to provide any documentation to show that collection efforts were made.

- Of the PAUR hospital provider cases we tested, two identified overpayments. In each of these cases, or 100 percent, follow-up collection procedures were not followed.

Criteria

To comply with the Virginia Debt Collection Act, Code of Virginia §2.2-4800-4809 and the federal requirement to seek recovery of payments, 42 CFR §455.16(a)(3), Medical Assistance Services established procedures to send overpayment notice letters and invoicing letters and pursue collection of overpayments from recipients and providers within specified timeframes. Overpayment notice letters inform recipients and providers to respond within 30 days by writing a check, setting up a repayment plan, or appealing the overpayment notice. If the recipient or provider does not respond, the Accounts Receivable Unit establishes a receivable in the agency's financial system and sends an invoice letter to the recipient or provider. At 30 days past the due date established in the invoice letter, the Accounts Receivable Unit establishes a negative balance in its claims processing system for amounts owed by providers. At 60 days past the due date established in the invoice letter, the Accounts Receivable Unit refers the receivable to the Virginia Department of Taxation and to the Commonwealth's collection agency (if less than $3,000) or the Office of the Attorney General (if $3,000 or more).

Consequence

By not following internally established procedures designed to meet Commonwealth and federal requirements, Medical Assistance Services is potentially not collecting money owed from recipients and providers. Untimely fiscal transactions may potentially damage Medical Assistance Services' credibility with other entities that it is dependent on for financial resources.

Cause

According to management, since fiscal year 2015, the Accounts Receivable Unit has been understaffed, which resulted in a backlog in the Accounts Receivable area. Current staff are only able to focus on the new receivable balances and are not able to work on clearing the existing backlog of past due amounts. Additionally, the implementation of an automated overpayment processing function has

been delayed due to a shift in priorities to upgrade the current financial system and replace the current claims processing system.

Recommendation

Medical Assistance Services should allocate appropriate resources to pursue collections and to ensure they are performed timely and accurately. This may be accomplished through the continued development of the automatic overpayment processing function and/or addressing staffing limitations. Medical Assistance Services should also ensure that sufficient claim information and consistent procedures are being communicated from the Program Integrity Division to the Accounts Receivable Unit in order to facilitate accurate and timely pursuit and reporting of overpayment collections.

Why the APA Audits Compliance with the Statement of Economic Interest Requirements

Medical Assistance Services has designated over one hundred employees in a position of trust. The Code of Virginia requires all individuals in a designated position of trust to complete the Statement of Economic Interest Disclosure Forms and complete the related training. To evaluate Medical Assistance Services' compliance with the Code of Virginia, we compared its practices to those required by the Code of Virginia.

Create Policies and Procedures to Ensure Compliance with Statement of Economic Interest Requirements

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Condition

Medical Assistance Services did not ensure the employees it designated as occupying a position of trust completed the required Statement of Economic Interest form. Specifically, six employees designated as required filers did not file in accordance with the Code of Virginia. Each of the six employees were either hired or transferred into positions of trust, requiring them to complete a Statement of Economic Interest form upon assuming the position. Five additional employees designated as required filers did not complete the required Statement of Economic Interest training within the required timeframe.

Criteria

Pursuant to the Code of Virginia §2.2-3114A and §2.2-3118.2, persons occupying positions of trust within state government shall file with the Ethics Council, as a condition to assuming office or employment, a disclosure statement of their personal interests and such other information as is required on the form, on or before the day such office or position of employment is assumed, and thereafter shall

file such a statement annually on or before February 1. Additionally, per the Conflict of Interest Act, filers must complete orientation training to help them recognize potential conflicts of interest. This orientation must be completed within two months of hire and at least once during each consecutive period of two calendar years.

Consequence

Medical Assistance Services could be susceptible to actual or perceived conflicts of interest that would impair or appear to impair the objectivity of certain programmatic or fiscal decisions made by employees in designated positions of trust. By failing to ensure that all required employees have completed the necessary disclosures and training, Medical Assistance Services may be prevented from relying on its employees to effectively recognize, disclose, and resolve conflicts of interest. While not a cost to Medical Assistance Services, employees in a position of trust who do not complete the required Statement of Economic Interest form may, as allowed by the Code of Virginia §2.2-3124, be assessed a civil penalty in an amount equal to $250.

Cause

Medical Assistance Services' Human Resources Division does not have written policies and procedures to guide management through the Statement of Economic Interest process, including the determination of who should be a required filer. In addition, the Human Resources Division did not adequately monitor employees or hold them accountable for compliance with Statement of Economic Interest requirements.

Recommendation

The Human Resources Division should create, implement, and maintain written policies and procedures to meet Code of Virginia requirements for the Statement of Economic Interest. These policies should incorporate guidance issued by the Commonwealth's Ethics Council. Additionally, as required by the Code of Virginia, the Human Resources Division should monitor all employees designated in a position of trust to ensure they complete the required Statement of Economic Interest training once within each consecutive period of two calendar years and maintain a record of such attendance.

Department of Social Services

Why the APA Audits Information System Security

Social Services is responsible for managing federally mandated eligibility programs for the Commonwealth of Virginia, such as Temporary Assistance for Needy Families (TANF), Supplemental Nutrition Assistance Program (SNAP), Medicaid, and Child Support Services. In order to manage the significant volume of personal and financial data, Social Services relies on IT systems for the collection, management, and storing of data. Due to the sensitivity of the data, appropriate policies, procedures, and security controls in accordance with the Security Standard, federal regulations, and industry-specific best practices must be in place to ensure its protection from malicious intent and disastrous events. To evaluate the controls surrounding information systems, we compared the practices of Social Services to those required by the Security Standard.

Improve Database Security for Financial Reporting System

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Condition

Social Services does not secure the database supporting its financial reporting system in accordance with the Security Standard and industry best practices. We identified five control weaknesses and communicated the details of these weaknesses to management in a separate document marked FOIAE under §2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls.

Criteria

The Security Standard requires agencies to implement certain minimum controls to safeguard data that is stored in database systems. This serves to reduce unnecessary risk to data confidentiality, integrity, and availability.

Consequence

By not implementing the controls discussed in the FOIAE communication, the system's database is not secure against known vulnerabilities. This increases the risk for malicious users to exploit those vulnerabilities and compromise sensitive Commonwealth data.

Cause

Social Services' lack of necessary resources contributed to the weaknesses in the database. In addition, Social Services lacks enterprise-wide processes to implement consistent settings and controls throughout the database environments.

Recommendation

Social Services should allocate the necessary resources to ensure that database configuration, settings, and controls align with the requirements in the Security Standard and industry best practices, such as the CIS Benchmark. Additionally, Social Services should consistently implement controls across all of its systems. Doing this will help maintain the confidentiality, integrity, and availability of sensitive and mission critical data.

Continue Improving Database Security for Case Management System
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Partial, with limited progress in this area

Condition

Social Services continues to test corrective actions to improve security controls over the database supporting its case management system in accordance with the Security Standard and industry best practices. We identified four control weaknesses and communicated the details of these weaknesses to management in a separate document marked FOIAE under §2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls.

Criteria

The Security Standard requires agencies to implement certain minimum controls to safeguard data that is stored in database systems. This serves to reduce unnecessary risk to data confidentiality, integrity, and availability.

Consequence

By not implementing the controls discussed in the FOIAE communication, the system's database is not secure against known vulnerabilities. This increases the risk for malicious users to exploit those vulnerabilities and compromise sensitive Commonwealth data.

Cause

Social Services is testing settings and configurations to resolve the weaknesses in the database and has plans to implement the corrective actions by the end of calendar year 2017. Due to storage capacity issues, Social Services experienced delays implementing a tool to resolve two specific identified

weaknesses; additionally, it lacked the necessary resources to resolve all prior year weaknesses in a timely manner.

Recommendation

Social Services should dedicate the necessary resources to ensure database configuration, settings, and controls align with the requirements in the Security Standard and industry best practices, such as the Center for Internet Security Benchmark. Doing this will help maintain the confidentiality, integrity, and availability of sensitive and mission critical data.

Improve Policies, Procedures, and Plans for Backup and Restoration
Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes

Condition

Social Services continues to not update its policies and procedures for backup and restoration to reflect the current process. Specifically, the Business Impact Analysis (BIA) includes Recovery Point Objectives (RPOs), but the continuity planning documents do not include RPOs. Additionally, the backup and recovery services provided by the IT Partnership do not support the RPOs identified by the business owners. Furthermore, Social Services has not documented and approved its backup and restoration plans.

Criteria

The Security Standard, section CP-9, requires an agency to conduct backups in the information system in accordance with the organization-defined frequency consistent with recovery time and recovery point objectives. Section CP-9-COV of the Security Standard requires that an agency develop and implement documented backup and restoration plans to support the restoration of systems, data, and applications in accordance with agency requirements. Additionally, the Security Standard, section 3.2, requires that an agency document the RPOs for each system required to recover a mission essential function or primary business function.

Consequence

Without maintaining robust IT risk management plans and contingency plans that accurately reflect the current process, Social Services may not be able to consistently govern the Partnership's backup and restoration efforts to meet operational needs. Without formal, approved backup and restoration plans, Social Services may not be able to successfully restore mission essential functions that are dependent on software applications after system failure.

Cause

The business recovery needs do not align with the current backup and restoration processes. This is due to Social Services lacking resources and other competing priorities within the IT environment.

Recommendation

Social Services should allocate the necessary resources to align its IT risk management plans (BIA and Risk Assessments) and IT contingency plans (Continuity of Operations and IT Disaster Recovery Plan) with the current backup and restoration process. While revising the documents, Social Services should clearly delineate the recovery time and recovery point objectives for the mission essential and primary business functions and the supporting IT systems. Furthermore, if there are variances in recovery time and recovery point objectives between the business function and IT system, Social Services should obtain formal acknowledgement of acceptance from business owners and documented manual workarounds the business function will perform until the IT system is recovered.

Why the APA Audits Management's Use of Third-Party Service Provider Audit Reports

Social Services uses several third-party service providers to facilitate the collection and storage of financial and protected personally identifiable information that is material to the Commonwealth's financial statements and federal programs. While these services are not directly performed by Social Services, Social Services must maintain oversight by ensuring that the internal control environment established by the third-party service providers is consistent with the services in the contract and the Security Standard to safeguard the sensitive data against potential threats. To ensure that Social Services is properly monitoring third-party service providers, we evaluated whether management was properly obtaining, reviewing, and reacting to their service provider audit reports.

Continue Improving Oversight of Third-Party Service Providers

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: Yes

Condition

Social Services continues to develop a formal process to maintain oversight over third-party IT service providers (providers). Social Services has outsourced several of its mission critical business functions, such as IT services, Child Support Enforcement call centers, and benefits administration services.

Criteria

The Security Standard, section 1.1, states management remains accountable for maintaining compliance with the Security Standard through documented agreements with providers and oversight

of services provided. Additionally, the Commonwealth's Hosted Environment Information Security Standard (Hosted Security Standard), section SA-9-COV-3, requires Social Services to perform a security audit or review an audit report of the provider's environment on an annual basis.

Consequence

Without an established process to gain assurance over providers' internal controls, Social Services cannot consistently validate that those providers have effective security controls to protect its sensitive data.

Cause

Since the prior year audit, Social Services developed a formal policy to maintain oversight over providers and developed contract language to include in all contracts with providers. Prior to implementing the formal policy, Virginia Information Technologies Agency (VITA) began its Enterprise Cloud Oversight Services (ECOS) that all executive branch agencies must use for providers that meet certain criteria. Social Services consulted with VITA to determine which providers must use ECOS, delaying Social Services from implementing an internal oversight process for providers that do not qualify for ECOS.

Recommendation

Social Services should continue developing a formal process for gaining appropriate assurance over outsourced operations that affect its IT environment, sensitive data, or mission critical processes. Social Services can obtain assurance in several forms including, but not limited to, Service Organization Control reports, on-site reviews, or other independently verified assurance of the provider's internal control environment. Additionally, Social Services should maintain oversight of this process to confirm compliance with requirements outlined in the Security Standard, Hosted Security Standard, and industry best practices.

Why the APA Audits Compliance with the Statement of Economic Interest Requirements

Social Services has designated over 20 employees in a position of trust and some of these employees negotiate and award multi-million dollar contracts on behalf of the Commonwealth. The Code of Virginia requires all individuals in a designated position of trust to complete the Statement of Economic Interest Disclosure Form and related training. To evaluate Social Services' compliance with the Code of Virginia, we compared its practices to those required by the Code of Virginia.

Obtain and Retain Statement of Economic Interest Training Records

Type: Internal Control and Compliance
Severity: Significant Deficiency
Repeat: No

Condition

Social Services' Statement of Economic Interest Coordinator is not ensuring that employees within a position of trust complete the required Statement of Economic Interest training every two years. In addition, Social Services is not maintaining records of training attendance as required.

Criteria

The Code of Virginia §2.2-3128 through 3131 requires that each Statement of Economic Interest filer complete Conflict of Interest Act training at least once every two years. This training is designed to help filers recognize potential conflicts of interest. As of December 1, 2015, the Ethics Council offers an orientation video on their website, which satisfies this requirement. Filers who register and watch the entire video get credit for taking the training. As required by §2.2-3129, each agency must maintain, for a minimum of five years, records of who completed the orientation course.

Consequence

Social Services cannot ensure that its employees are completing the training as required and may be limited in its ability to hold its employees accountable for not knowing how to recognize a conflict of interest and how to resolve it. Additionally, filers could be subject to penalties for inadequate disclosure as outlined at §2.2-3120 through §2.2-3127.

Cause

The Social Services' Statement of Economic Interest Coordinator was not aware of the Code of Virginia requirement to maintain Statement of Economic Interest training records. Additionally, he was not aware that he had access to training records now that the Ethics Council offers the training.

Recommendation

The Statement of Economic Interest Coordinator should obtain and retain Statement of Economic Interest training records as required by the Code of Virginia. Social Services should use these records to ensure that employees in positions of trust complete the training once within each consecutive period of two calendar years. Additionally, Social Services should maintain the attendance records for a minimum of five years.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 15, 2017

The Honorable Ralph S. Northam
Governor of Virginia

The Honorable Robert D. Orrock, Sr.
Chairman, Joint Legislative Audit
and Review Commission

We have audited the financial records and operations of the **Agencies of the Secretary of Health and Human Resources**, as defined in the Audit Scope and Methodology sections below, for the year ended June 30, 2017. 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.

Audit Objectives

Our audit's primary objective was to evaluate the accuracy of the Agencies of the Secretary of Health and Human Resources' financial transactions as reported in the Comprehensive Annual Financial Report for the Commonwealth of Virginia for the year ended June 30, 2017, and test compliance for the Commonwealth's Single Audit (Single Audit). In support of this objective, we evaluated the accuracy of recorded financial transactions in the Commonwealth's accounting and financial reporting system, in each agency's accounting records and other financial information reported to the Department of Accounts; reviewed the adequacy of their internal control; tested for compliance with applicable laws, regulations, contracts, and grant agreements; and reviewed corrective actions of audit findings from prior year reports.

Audit Scope and Methodology

Management of the Agencies of the Secretary of Health and Human Resources 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 significance and risk in determining the nature and extent of our audit procedures. Our review encompassed controls over the following significant cycles, classes of transactions, and account balances at these four agencies:

Department of Behavioral Health and Developmental Services

- Accounts receivables
- Fixed asset management
- Operational expenses
- Payroll expenses
- Institutional revenues
- Community Service Board contracts
- Information system security
- Systems access controls
- Commonwealth's retirement benefit system
- Licensing behavioral health providers

Department of Health

- Accounts receivable
- Inventory
- Federal revenues, expenses, and compliance for:
  - Child and Adult Care and Feeding Program (CACFP)
  - Preventive Health and Health Services (PHHS)
- Payroll expenses
- Rescue squad support
- Collection of fees for services
- Cooperative agreements between Health and local government, including:
  - Aid to and reimbursement from local governments
  - Cost allocations
  - Accounts payable
- Information system security
- Systems access controls

Department of Medical Assistance Services

- Federal revenues, expenses, and compliance for:
  - Medicaid Cluster
  - Children's Health Insurance Program
- Accounts receivable
- Accounts payable
- Contract management
- System access controls
- Utilization units

Department of Social Services

Federal revenues, expenses, and compliance for:
- Child Support Enforcement
- Child Care Development Fund Cluster

Eligibility for:
- Medicaid
- Temporary Assistance for Needy Families
- Low Income Heating and Energy Assistance
- Child Care and Development Fund

Budgeting and cost allocation
Network and system security
Systems access controls
Child Support Enforcement asset accuracy
Supplemental Nutrition Assistance Program supplemental information
Accounts payable

The following agencies under the control of the Secretary of Health and Human Resources are not material to the Comprehensive Annual Financial Report for the Commonwealth of Virginia. As a result, these agencies are not included in the scope of this audit.

Department for Aging and Rehabilitative Services
Department for the Blind and Vision Impaired
Department for the Deaf and Hard-of-Hearing
Department of Health Professions
Office of Children's Services
Virginia Board for People with Disabilities
Virginia Foundation for Healthy Youth
Virginia Rehabilitation Center for the Blind and Vision Impaired
Wilson Workforce and Rehabilitation Center

We performed audit tests to determine whether the agencies' 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; re-performance of automated processes; inspection of documents, records, and contracts; and observation of the agencies' operations. We performed analytical procedures, including budgetary and trend analyses. Where applicable, we compared an agency's policies to best practices and the Commonwealth's Information Security Standard. We also tested details of transactions to achieve our 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.

Conclusions

We found that the Agencies of the Secretary of Health and Human Resources, as defined in the Audit Scope and Methodology section above, properly stated, in all material respects, the amounts recorded and reported in the Commonwealth's accounting and financial reporting system, each agency's accounting records and in other information reported to the Department of Accounts for inclusion in the Comprehensive Annual Financial Report for the Commonwealth of Virginia.

Our consideration of internal control was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies; and therefore, material weaknesses and significant deficiencies may exist that were not identified. However, as described in the section titled "Internal Control and Compliance Findings and Recommendations," we identified deficiencies in internal control that we consider to be material weaknesses and other deficiencies that we consider to be significant deficiencies in internal control.

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 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 information or material non-compliance with provisions of a major federal program will not be prevented or detected and corrected on a timely basis. We have explicitly identified five findings in the section titled "Internal Control and Compliance Findings and Recommendations" that we consider to be material weaknesses for the Commonwealth.

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. We have explicitly identified 21 findings in the section titled "Internal Control and Compliance Findings and Recommendations" as significant deficiencies for the Commonwealth.

As the findings noted above have been identified as material weaknesses or significant deficiencies for the Commonwealth, 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 Financial Statements Performed in Accordance with Government Auditing Standards," included in the Single Audit Report for the year ended June 30, 2017. Certain findings relate to federal programs; as such, these findings will be reported in 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 is also included in the Single Audit Report for the year ended June 30, 2017. The Single Audit will be available on APA's website at www.apa.virginia.gov in February 2018.

In addition to the material weaknesses and significant deficiencies, we detected deficiencies in internal control that are not significant to the Commonwealth's Comprehensive Annual Financial Report and Single Audit, but are of sufficient importance to warrant the attention of those charged with

governance. We have explicitly identified two findings in the section titled "Internal Control and Compliance Findings and Recommendations" as deficiencies.

The Agencies of the Secretary of Health and Human Resources have taken adequate corrective action with respect to audit findings reported in the prior year that are not referenced as "repeat" findings in the section titled "Internal Control and Compliance Findings and Recommendations."

Exit Conference and Report Distribution

We discussed this report with management for the agencies included in our audit as we completed our work on each agency. Management's responses to the findings identified during our audit are included in the section titled "Agency Responses." We did not audit management's responses and, accordingly, we express no opinion on them.

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.

AUDITOR OF PUBLIC ACCOUNTS

LCW/alh

JACK BARBER, M.D.
INTERIM COMMISSIONER

COMMONWEALTH of VIRGINIA

DEPARTMENT OF
BEHAVIORAL HEALTH AND DEVELOPMENTAL SERVICES
Post Office Box 1797
Richmond, Virginia 23218-1797

Telephone (804) 786-3921
Fax (804) 371-6638
www.dbhds.virginia.gov

MEMORANDUM

TO: Ms. Martha Mavredes - Auditor of Public Accounts

FROM: Jack Barber, M.D. JWB

SUBJECT: *Responses to FY 2017 HHR Report*

DATE: December 12, 2017

The purpose of this memo is to provide the Department of Behavioral Health and Developmental Services (DBHDS) responses to the management comments listed in the HHR report. The following are the responses:

Continue to Improve IT Governance – REPEAT:

DBHDS concurs with the comment. DBHDS acquired funds and contracted with Gartner to help provide remediation actions for this finding. Outdated technology/applications were identified. An overarching DBHDS Governance structure/process has been put in place, not only for the IT applications, but also for IT Security to be engaged from the beginning. The Governance Executive Committee consists of all the Deputy/Assistant Directors as well as all DBHDS Facility Directors. The Governance Committee will address new projects as well as consider whether previously identified facility applications should be considered for conversion to enterprise applications. The funding request to hire additional staff resources (Project Managers/Business Systems Analysts) to fully support the governance process was approved. Job descriptions have been created and hiring will start in January 2018. The net result will be a significant reduction in the number of duplicate applications, a decrease in the cost to support and secure the applications, and a subsequent increase in the quality of application support and function provided to the agency's business units. Additionally, the reduction in DBHDS sensitive IT systems will continue. The estimated completion date for this response is June 30, 2018.

Improve IT Contingency Management Program:
DBHDS concurs with the comment. DBHDS has started an IT COOP / DRP project with a projected completion date of October 1, 2018. This project will develop procedures, assign roles and responsibilities, and update the IT COOPs and DRPs ensuring they are consistent across the agency. DBHDS will ensure these IT COOPs and DRPs are tested annually. The implementation of this response may be contingent on securing additional resources.

Continue to Upgrade Unsupported Technology – REPEAT:
DBHDS concurs with the comment. DBHDS has submitted a security exception to Commonwealth Security to upgrade, consolidate, or decommission all end-of-life/end-of-support technology by March 31, 2018.

Develop Baseline Configurations for Information Systems – REPEAT:
DBHDS concurs with the comment. DBHDS will complete the installation of server software by March 31, 2018, which will establish and maintain security baseline configurations for our sensitive information systems. This software will ensure we meet the requirements of the Commonwealth's Security Standards.

Increase Oversight over Third Party Providers - REPEAT:
DBHDS concurs with the comment. DBHDS Information Security is developing a formal process to gain assurance that their third party providers have secure IT environments to protect sensitive data. This process will be incorporated into the Information Security program and will be complete by July 1, 2018.

Improve Internal Controls over Capital Asset Additions - REPEAT:
DBHDS concurs with the comment. DBHDS will continue to work toward compliance regarding the accuracy and timeliness of the recording of fixed assets at all facilities and Central Office. In addition, policies over fixed assets will be enhanced to cover the areas noted in the audit. The estimated completion date for this response is June 30, 2018.

Improve Internal Controls over Reconciliations:
DBHDS concurs with the comment. DBHDS Central Office will work to ensure that all facilities reconcile FAACS, FMS and CARDINAL and AVATAR, CARDINAL and FMS; accurately, completely and timely with indication of the preparer and approver of the reconciliation. The estimated completion date for this response is June 30, 2018.

Improve Controls Over the Commonwealth's Retirement Benefits System – REPEAT:
The Department concurs with the audit comment and will ensure the following steps are taken to address the issues noted in the management comment:

- Exceptions identified on the Commonwealth's payroll system automated reconciliation reports will be cleared timely by all DBHDS facilities and Central Office. In addition,

reconciling items on the creditable compensation reconciliation will be cleared prior to certifying the snapshot.

- All DBHDS facilities and Central Office will maintain adequate documentation showing that there is a regular review of the Commonwealth's human resource system cancelled records reports and any exceptions noted on the report will be cleared timely.

- All DBHDS facilities and Central Office will perform reconciliations of creditable compensation between *my*VRS Navigator and the Commonwealth's human resource system. This will be done by utilizing reports with specific information regarding creditable compensation.

- All DBHDS facilities and Central Office will continue to work to ensure that access to *my*VRS Navigator is deleted timely after a user terminates employment. The goal will be to delete access within three business days after someone leaves employment.

- Policies and procedures in place at all DBHDS facilities and Central Office will be enhanced to include instructions for reconciling creditable compensation items between PMIS and *my*VRS Navigator prior to confirming the snapshot.

To help with completing these responses the following will be put into place:

- A revised VNAV reconciliation policy/procedure was sent out to all DBHDS HR managers on October 25, 2017.

- All DBHDS facilities were asked to submit their revised VNAV reconciliation procedures by December 1, 2017.

- Training on the VNAV reconciliation will be given to HR staff on December 15, 2017 at the DBHDS HR Forum.

The VNAV reconciliation will be added to the ARMICS work completed by all DBHDS facilities and Central Office.

Improve Controls Over Payroll:

The Department concurs with the audit comment. The DBHDS Office of Internal Audit conducted this testwork and has reviewed the responses to the findings that were given by the facilities tested. The Department has agreed with the responses to the findings and will be completing follow-up reviews to ensure compliance. The estimated completion date for this response is September 1, 2018.

Please let me know if you have any questions about the information we have provided.

cc: Jack Barber, M.D., DBHDS Interim Commissioner

Kathy Drumwright, DBHDS Interim Chief Deputy Commissioner
Connie Cochran, DBHDS Deputy Commissioner for Developmental Services
Don Darr, DBHDS Assistant Commissioner for Finance and Administration
Daniel Herr, DBHDS Deputy Commissioner for Behavioral Health
Dev Nair, DBHDS Assistant Commissioner for Quality Management and Development
Michael Schaefer, Ph.D; DBHDS Assistant Commissioner for Forensic Services
Greg Bell, DBHDS Chief Information Security Officer
Andrew Diefenthaler, DBHDS Assistant Director of Finance and Administration
Ken Gunn, DBHDS Director of Budget and Financial Reporting
Dan Hinderliter, DBHDS Director of the Office of Administrative Services
Stacy Pendleton, DBHDS Assistant HR Director
Chris Sarandos, DBHDS Chief Information Officer
Randy Sherrod, DBHDS Internal Audit Director

COMMONWEALTH of VIRGINIA

Department of Health

Marissa J. Levine, MD, MPH, FAAFP
State Health Commissioner

P O BOX 2448
RICHMOND, VA 23218

TTY 7-1-1 OR
1-800-828-1120

January 29, 2018

Martha S. Mavredes, CPA
Auditor of Public Accounts
P.O. Box 1295
Richmond, VA 23218

Dear Ms. Mavredes:

We have reviewed your report on our audit for the year ended June 30, 2017. We concur with the findings, and a copy of our corrective action plan has been provided under a separate cover memo.

We appreciate your team's efforts and constructive feedback. Please contact Alvie Edwards, Internal Audit Director, if you have any questions regarding our corrective action plan.

Sincerely,

Marissa J. Levine, MD, MPH, FAAFP
State Health Commissioner

VDH VIRGINIA DEPARTMENT OF HEALTH
Protecting You and Your Environment
www.vdh.virginia.gov

COMMONWEALTH of VIRGINIA

Department of Medical Assistance Services

SUITE 1300
600 EAST BROAD STREET
RICHMOND, VA 23219
804/786-7933
804/225-4512 (Fax)
800/343-0634 (TDD)

January 17, 2018

Ms. Martha S. Mavredes
The Auditor of Public Accounts
P. O. Box 1295
Richmond, Virginia 23218

Dear Ms. Mavredes:

We have reviewed your draft audit report findings for the Department of Medical Assistance Services (DMAS) to be included in the report for the Audit of the Agencies of the Secretary of Health and Human Resources for the Fiscal Year Ending June 30, 2017. We concur with the audit findings assigned to DMAS. Attached please find the Department's Corrective Action Plan for the DMAS FY 2017 audit findings.

If you have any questions or require additional information, please do not hesitate to contact our Internal Audit Director, Paul Kirtz.

Sincerely,

Jennifer Lee, M.D.
DMAS Director

Department of Medical Assistance Services
APA Audit of the DMAS for the Fiscal Year Ending June 30, 2017
Corrective Action Plan
January 17, 2018

Develop Processes to Facilitate the Controlling of Privileges in the Claims Processing System (issued as MP#7)

Condition

Medical Assistance Services' Office of Compliance and Security (Compliance and Security) completed a conflict matrix documenting certain combinations of privileges that create internal control weaknesses in its Current System. However, the conflict matrix does not document all combinations of over 900 capabilities within the Current System that may create internal control weaknesses.

Recommendation

Medical Assistance Services should continue to perform manual access reviews and review for violations of the concept of segregation of duties and the principle of least privilege within the Current System. In addition, Compliance and Security should gain an understanding of the security environment in the New Claims Processing System and ensure it establishes a process to document and evaluate system access by completing a conflict matrix and incorporating the documentation into the annual access evaluation process.

Corrective Action Plan:

DMAS will continue to perform the manual access reviews of its Current Claims Processing System and will review for conflicts of segregation of duties and ensure that users have the proper role needed for their responsibilities.

The replacement for the Current Claims Processing System (i.e. the New Claims Processing System) will emphasize profile and role-based security. All profiles and roles will be documented in business terms, including a conflict matrix, so that managers, security and IT can clearly see what is being granted and what cannot be granted in combinations. Profiles and role base security will be implemented as each New Claims Processing System module is implemented. All New Claims Processing System components are expected to be implemented by March 31, 2020.

Responsible Persons:

- Mukundan Srinivasan, DMAS Chief Information Security Officer, Information Management Division
- Bill Burnette, DMAS Acting Information Security Officer, Office of Compliance and Security

Estimated Implementation Date: March 31, 2020

Remove Access to the Current Claims Processing System in a Timely Manner (issued as MP#5)

Condition

Medical Assistance Services did not remove access to the Current System for individuals who no longer needed access. Specifically, eight of 16 of the separated employees listed on the access report did not have their access suspended within 24 business hours. The eight employees in question retained their unsuspended access between seven and 34 days after separation.

Recommendation

Compliance and Security and the Human Resources Division should establish effective, regular communication to report staff changes to those individuals responsible for managing system access. In addition, Compliance and Security should ensure compliance with its Access Control Policy and the Security Standard by removing users' access as required.

Corrective Action Plan:

Currently, the process for removing an individual's Current Claims Processing System access is a completely manual process. DMAS is in the process of developing an automated workflow process for termination of system access. Termination notices will be communicated directly to the Office of Compliance and Security (OCS) by the employee's manager. OCS will have a daily dashboard of employees to be removed from the system. OCS projects this process will be implemented by March 1, 2018.

Responsible Persons:

- Mukundan Srinivasan, DMAS Chief Information Security Officer, Information Management Division
- Bill Burnette, DMAS Acting Information Security Officer, Office of Compliance and Security

Estimated Implementation Date: March 1, 2018

Complete Annual Review for the Current Claims Processing System (issued as MP#6)

Department of Medical Assistance Services
APA Audit of the DMAS for the Fiscal Year Ending June 30, 2017
Corrective Action Plan
January 17, 2018

Medical Assistance Services' Compliance and Security did not complete an annual access review for one of the three user groups of the Current System. Compliance and Security completed an annual access review of the Virginia Department of Social Services (Social Services) and contractors user groups; however, it did not perform an annual review of Medical Assistance Services employees. The most recent review of Medical Assistance Services employees' system access was completed in April 2016. As of August 1, 2017, Compliance and Security had not started its review of Medical Assistance Services employees.

Recommendation

Compliance and Security should perform an annual review of its employees' access to the Current System in order to identify unnecessary access due to terminations or changes in job responsibilities. In addition, Compliance and Security should ensure compliance with the Security Standard and ensure its policy identifies the specific time in which the annual review should occur.

Corrective Action Plan:

DMAS completed the annual user access review in October 2017 and will emphasize the timing of the review to ensure that we complete user access reviews every 12 months. Managers have become more accustomed to the process and are responding faster. DMAS will develop a schedule for user access reviews to incorporate in its policy and procedures to ensure that the review cycle is in compliance with the Security Standard.

The process remains manual, DMAS plans to automate the process within the New Claims Processing System. We also intend to improve the process with the implementation of a risk management software and with VITA's Active Directory migration.

Responsible Persons:

- Mukundan Srinivasan, DMAS Chief Information Officer, Information Management Division;
- Bill Burnette, DMAS Information Security Officer, Office of Compliance and Security

Estimated Implementation Date: June 30, 2018

Perform the Required Information Technology Review (issued as MP#10)

Condition

Department of Medical Assistance Services
APA Audit of the DMAS for the Fiscal Year Ending June 30, 2017
Corrective Action Plan
January 17, 2018

Since January 31, 2014, the Medical Assistance Services has not completed the required biennial Automated Data Processing (ADP) risk analyses and system security review. In January 2017, Medical Assistance Services' Internal Audit Division contracted with an external service provider to perform the required security review of the Current System. However, the review has not been finalized, and Medical Assistance Services has not received a final report from the external service provider as of October 2017.

Recommendation

Medical Assistance Services should ensure that the required biennial review is completed and that future reviews are completed and are arranged to meet the timing and other requirements. In addition, Medical Assistance Services should use the results of these reviews to ensure its provider complies with the requirements in the Security Standard, Commonwealth Accounting Policies and Procedures (CAPP) Manual, Code of Federal Regulation, and contract with the Commonwealth. If weaknesses are disclosed from the required review, Medical Assistance Services should implement complementary controls to mitigate the risk to the Commonwealth until the provider corrects the deficiency.

Corrective Action Plan:

DMAS concurs that the Agency did not conduct a security audit of the Current Claims Processing System in the two-year cycle as required pursuant to 45 CFR §95.621. The delay in the biennial audit was due to the U. S. Department of Health and Human Services - Office of Inspector General (OIG) conducting a comprehensive security audit of the Current Claims Processing System that started in September 2015. The OIG auditors used 45 CFR §95.621 – Automated Data Processing System Security Requirements and Review Process as criteria for the audit. In the OIG fieldwork exit conference presentation was held on April 28, 2016.

DMAS received the final audit report from the OIG on April 25, 2017. DMAS and the Service Provider have been working to address the audit issues and system vulnerabilities noted in the audit.

Due to strained resources for both the Service Provider and DMAS in responding to the audit requests and resolving the audit issues, we choose not to begin another similar security audit while the OIG was still performing its audit fieldwork and testing. In arriving at this decision, consideration was given to preventing duplication of effort for limited resources. Additionally, the results of the OIG audit provide helpful insight to efficiently develop the scope of the DMAS security audit of the Current Claims Processing System.

DMAS worked with Computer Aid, Inc. (CAI) through the COV IT Contingent Labor Contract (Statement of Work Process) to obtain IT services (Security Audits) from a CAI subcontractor. DMAS provide the Statement of Requirements to CAI on September 15,

2016. After reviewing the SOW submitted by the CAI subcontractor, DMAS selected the subcontractor and began negotiating the Statement of Requirements which delayed the start of the audit.

The contract between CAI and DMAS was executed on January 23, 2017. The Current System IT Security Audit fieldwork, testing, documentation, and report preparation began after the entrance conference on March 22, 2017 and was completed in October 2017.

The results of the OIG Current Claims Processing System Security Audit and the CAI Subcontractor Current Claims Processing System IT security audit will assist DMAS in monitoring the Service Provider to ensure compliance with the Commonwealth Security Standard, CAPP Manual, Code of Federal Regulation, and the contract with the Commonwealth. If any weaknesses are identified in the audits, DMAS will implement complementary controls to mitigate the risk to the Commonwealth until the Service Provider corrects the deficiency.

The following milestones for the Current Claims Processing System IT Security Audit project completed the corrective action:

- The CAI subcontractor issued its draft Current Claims Processing System IT Audit Report on October 18, 2017.
- DMAS provided responses to the findings on November 17, 2017. Responses were reviewed by Internal Audit and provided to the CAI subcontractor for incorporation into the final report.
- The CAI subcontractor provided the final audit report to Internal Audit on November 30, 2017 for review.
- Internal Audit distributed the final audit report to DMAS management on December 8, 2017 and discussed with the DMAS Director on December 14, 2017.

Corrective Action Plans for the recommendations were added to our quarterly tracking of CAP status updates beginning in CY 2018.

Responsible Persons:

- Paul Kirtz, DMAS Internal Audit Director, Internal Audit Division
- Mukundan Srinivasan, DMAS Chief Information Officer, Information Management Division;
- Bill Burnette, DMAS Acting Information Security Officer, Office of Compliance and Security

Implementation Date: Corrective Action for the finding was completed on December 14, 2017.

Review and Document Service Organization Control Reports of Third-Party Service Providers (issued as MP#9)

Condition

Medical Assistance Services does not review each of its third-party service providers' (providers) Service Organization Control reports. Providers are entities that perform outsourced tasks and business functions on behalf of Medical Assistance Services and the Commonwealth. A Service Organization Control report provides an independent description and evaluation of the provider's internal controls. Although Medical Assistance Services works closely with its providers, management should regularly review Service Organization Control reports and document the results of its reviews in order to ensure the effectiveness of providers' controls.

Recommendation

Medical Assistance Services should develop and implement policies and procedures to review, assess, and document the effectiveness of provider controls reported through Service Organization Control reports. In addition, Medical Assistance Services should use Service Organization Control reports as a component of its oversight activities over its providers to confirm they comply with the requirements outlined in the Security Standard, CAPP Manual, and industry best practices. If weaknesses are identified in Service Organization Control reports, Medical Assistance Services should implement complementary controls to mitigate the risk to the Commonwealth until the provider corrects the deficiency.

Corrective Action Plan:

Corrective Action Taken as of September 30th 2017:

1. Developed new guidelines and procedures in the IT procurement process:
   - Listing all required standards in RFP Template including SOC Reports and where to find detail.
   - Requiring SOC 2 Type 2 reports in contract requirements for the New Claims Processing System contracts.
   - Establishing reporting timelines for oversight activities when the system is live
     - SOC II, Type 2 – Initial report due within 90 days of contract effective date, thereafter due annually.

2. Completed following actions for SOC report reviews:
   - Developed a SOC report review questionnaire template

- Used the template to review SOC reports received from the Current Claims Processing System IT Contractor for its IT data center subcontractors
- Developed a SOC2 PowerPoint training explaining the SOC2 report, defining its purpose and how to review the document.

Corrective Actions to be completed:

Develop internal protocol with stakeholders, including PCM, Information Management, Contract Administrators and others as needed, to implement SOC receipt and review requirement for required DMAS contracts. Policies and Procedures to include:

- Coordination and responsibilities between, PCM, Contract Administrator and subject matter experts
- Language in contracts identified as having significant fiscal transactions through use of developed tool for the Contractor to provide appropriate SOC report on a regular basis
- Update semi-annual contractor performance evaluation form used by Contract Administrators to include as appropriate:
    1. Confirmation of receipt of annual SOC report (yearly) from contractor
    2. Confirmation of receipt of any Corrective Action Plan
- Include provisions for a DMAS mitigation plan for significant weaknesses found in SOC reports.

Responsible Persons:

- Mukundan Srinivasan, DMAS Chief Information Officer, Information Management Division;
- Bill Burnette, DMAS Acting Information Security Officer, Office of Compliance and Security
- Chris Foca, Division Director, Procurement and Contract Management

Estimated Implementation Dates: September 30, 2018

Ensure Employees have Proper Access Roles within the Commonwealth's Procurement System (issued as MP# 1)

Condition

Medical Assistance Services is not effective in ensuring that employees have proper access roles within the Commonwealth's procurement system. For the entire fiscal year 2017, Compliance and Security did not remove the previous Interim Director of the Procurement and Contract Management Division's "No Supervisor" role in the procurement system. Additionally, during this same time, the current Director of the

Procurement and Contract Management Division did not have the "No Supervisor" role in the procurement system. Users with the "No Supervisor" role may retrieve all requisitions for all employees in their chain of direct reporting in the procurement system.

Recommendation

Medical Assistance Services should ensure that employees only have access levels appropriate for them to perform their assigned job duties. In addition, Medical Assistance Services should utilize the assigned "Entity Lead" within the Procurement and Contract Management Division to communicate any necessary changes in access to the System Security Officer. The Entity Lead is an individual whose responsibilities would include working with the System Security Officer and the Department of General Services to ensure proper user access is established and maintained. This liaison between the procurement function and the System Security Officer would contribute to an environment where necessary changes to access are being regularly disseminated to the System Security Officer so they can be effective in ensuring that employees have proper access roles within the procurement system.

Corrective Action Plan:

In September 2017, the account with the 'No Supervisor' role in Commonwealth's procurement system was reassigned from the acting Procurement Manager to the current Procurement and Contract Management (PCM) Division Director.

The PCM Division Director or his designee will work as the "Entity Lead" with the System Security Officer and DGS to ensure that proper user access is established and maintained in Commonwealth's procurement system. The Entity Lead will disseminate changes in access roles to the System Security Officer. The System Security Officer will document a standard procedure of administering and reviewing user access and will work with the Entity Lead during the annual user access review.

The former DMAS ISO retired during the audit. The acting ISO will obtain Commonwealth procurement system training in order to understand and implement procurement system security requirements for DMAS. This will allow him to introduce effective review and revision procedures. The training will be scheduled during the first quarter of 2018 and DMAS OCS will begin directly administering the procurement system by March 31, 2018.

Responsible Persons:

- Mukundan Srinivasan, DMAS Chief Information Officer, Information Management Division
- Bill Burnette, DMAS Acting Information Security Officer, Office of Compliance and Security

Estimated Implementation Date: March 31, 2018

Correct Policies and Procedures for E-mailing Sensitive Information to State Agencies (issued as MP# 2)

Condition

Medical Assistance Services incorrectly instructed its employees that they did not have to use a data protection mechanism, encryption, when e-mailing sensitive information to another state agency. As a result, Medical Assistance Services' employees exchanged sensitive information within the agency and to other state agencies through unsecured, unencrypted e-mail.

Recommendation

Medical Assistance Services should develop and implement policies and procedures for its employees to transmit personally identifiable information securely and in accordance with the Security Standard. Medical Assistance Services should ensure that all employees understand their responsibility and monitor for compliance.

Corrective Action Plan:

DMAS will develop and implement policies, procedures for its employees to transmit personally identifiable information (PII) and protected health information (PHI) securely, by completing its corrective action steps. The steps contain information that is sensitive and confidential to the security of the system. Since this report and the response will be public information, the steps are not included in our response.

Once the steps are completed, we expect a comprehensive mail encryption solution to be available to users by the second quarter of 2018.

Responsible Persons:

- Mukundan Srinivasan, DMAS Chief Information Officer, Information Management Division
- Bill Burnette, DMAS Acting Information Security Officer, Office of Compliance and Security

Estimated Implementation Date: April 1, 2018

Develop Procedures and Performance Expectations for Resolving Social Security Number Discrepancies (issued as MP#4)

Condition

As of August 2017, the number of Medicaid recipients with Social Security Number (SSN) discrepancies that remain uncorrected after 12 months is 523. While this is an increase of 316 from the prior August, with just over one million individuals receiving Medicaid services, the 523 discrepancies represent one-twentieth of a percent of the total Medicaid population for Virginia. Monthly, Medical Assistance Services provides Social Services with all SSN discrepancies on the Social Security Number and Citizenship Report (RS-O-485A report) that require resolution.

Recommendation

Medical Assistance Services should provide Social Services with the RS-O-485A report every month. Additionally, Medical Assistance Services should create, implement, and maintain policies and procedures for the Social Security verification process. Finally, Medical Assistance Services should develop baseline performance expectations for Social Services related to resolving SSNs. Management of both Medical Assistance Services and Social Services should monitor performance and make adjustments, as needed, to meet expectations.

Corrective Action Plan:

Steps to be taken or that have been taken:

Provide VDSS with a copy of the RS-O-485A report each month

- For years, the Current Claims Processing System generated the RS-O485A report and it was sent to VDSS. However, the report did not contain the correct recipients. It contained Medicaid recipients and GAP cases but not FAMIS/FAMIS MOMS recipients. VDSS did not need the GAP cases but needed the Medicaid and FAMIS/FAMIS MOMS recipients. In March 2017, DMAS updated the RS-O-485A report to include both the Medicaid and FAMIS/FAMIS MOMS recipients began sending the report each month to VDSS. The March 2017 report included enrollment for January through March 2017. For the current process, the Office of Data Analytics generates the report and sends electronically to VDSS. DMAS is in the process of revising the RS-O-485A report so that the Current Claims Processing System will automatically generate the monthly report to include all Medicaid and FAMIS recipients (and not GAP cases) and automatically send it to VDSS.

Monitor completion of the RS-O-485A report each month

- Staff in the Enrollment Unit within the Division of Eligibility and Enrollment Services will monitor the report on a monthly basis to ensure that action has been taken to correct Social Security Numbers in the system. This action will begin in February 2018 and will be an ongoing monthly process. SSNs found to remain on the report and not corrected will be routed to the appropriate Virginia Department of Social Services Regional Medicaid Consultant for correction and provided to the Virginia Department of Social Services Medical Assistance Unit Manager.

Develop and implement policies, procedures and baseline performance measures related to Social Security numbers in the Current Claims Processing System.

- While there are policies and procedures related to verification of Social Security numbers already set out in the Medicaid eligibility manual, DMAS Eligibility and Enrollment Services Division Eligibility Policy Unit staff will update those current policies and procedures and develop baseline performance measures for local agency staff related to correction of numbers in the Current Claims Processing System. This will take place beginning in January 2018 with an expected implementation of no later than July 2018 and inclusion in the July 2018 Medicaid transmittal and Medicaid Eligibility Manual.
- DMAS Eligibility and Enrollment Services Division staff will work with staff from the Virginia Department of Social Services Medical Assistance Unit to implement these new procedures no later than July 2018 and will develop procedures for monitoring performance by local agencies no later than that date as well.

Responsible Persons:

- Cindy Olsen, Division Director, Eligibility and Enrollment Services Division

Estimated Implementation Date: July 1, 2018. Certain monitoring activities will be ongoing.

Improve Collective Knowledge of Annual Accrual Reporting (issued as MP#8)

Condition

Medical Assistance Services' Budget Division did not sufficiently explain why its Fiscal Division reported a one percent decrease in accrued claims as of fiscal year-end 2017, which is inconsistent with historical trends and the Budget Division's forecast for a ten percent increase in total claims expenditures for fiscal year 2018. Portions of fiscal year 2018 expenditures settle claims from fiscal year 2017.

Recommendation

Medical Assistance Services should ensure that, collectively, its Divisions have a sufficient understanding of the claims payable and related federal receivable accrual process. In addition, the Budget Division should actively collaborate with the Fiscal Division in order to provide the most accurate information to Accounts. Medical Assistance Services should create, implement, and maintain formal policies and procedures that provide sufficient direction for personnel to prepare the accrual schedules and to know when to question items that are outside of expected results and/or are not consistent with historical trends.

Corrective Action Plan:

DMAS will enhance formal policies and procedures that document the accrual process, including workflows, timelines, and resulting reports/documentation. In addition, DMAS will establish a review process to include an analysis of historical projections compared to actual accruals, identify unexpected inconsistencies, sufficiently explain variances and update projection data if needed. (Such policies, procedures and review will be completed prior to the next annual accrual submission, September 30, 2018.)

In addition, the Budget Division will institute an internal policy that informs Division staff how to effectively streamline audit responses and insure proper information is communicated with external audit staff. This corrective action will ensure that external audit staff receive complete and accurate information regarding accruals. (An email was sent by Budget Director on December 13, 2017 to all Budget Division staff outlining policy and a copy was saved to the Orientation folder on the Division's shared drive.)

Responsible Persons:

- Lanette Walker, Division Director, Budget Division

Estimated Implementation Date: All aspects of the corrective action plan will be completed prior to the next annual accrual submission due September 30th, 2018.

Improve Accounts Receivable Collection Process (issued as MP#13)

Condition

In certain cases, Medical Assistance Services Fiscal Division did not pursue collections from providers and recipients timely and in accordance with its policies and procedures. In certain cases tested from the Program Integrity Units, Medical Assistance Services' actions have resulted in a delay of possible collections. Specifically for each, we found:

- Of the Provider Review Unit cases we tested, seven identified overpayments. Within the seven, we found seven cases, or 100 percent, where the follow-up collection procedures were not followed.

- Of the Recipient Audit Unit cases we tested, 16 identified overpayments, 11 of which management determined collectable; however, in eight cases, or 73 percent, follow-up collection procedures were not followed.

- Of the Prior Authorization and Utilization Review (PAUR) mental health provider cases we tested, six identified overpayments, three of which management determined collectable; however, in one case, or 33 percent, management was not able to provide any documentation to show that collection efforts were made.

- Of the PAUR hospital provider cases we tested, two identified overpayments. In each of these cases, or 100 percent, follow-up collection procedures were not followed.

Recommendation

Medical Assistance Services should allocate appropriate resources to pursue collections and to ensure they are performed timely and accurately. This may be accomplished through the continued development of the automatic overpayment processing function and/or addressing staffing limitations. Medical Assistance Services should also ensure that sufficient claim information and consistent procedures are being communicated from the Program Integrity Division to the Accounts Receivable Unit in order to facilitate accurate and timely pursuit and reporting of overpayment collections.

Corrective Action Plan:

The untimely and inaccurate processing of accounts receivable transactions is directly associated with the delayed automation in overpayment processing, backlog of receivables, and the lack of appropriate resources to focus earnestly on collection efforts.

The Current Agency Accounting System upgrade was successfully implemented 11/13/2017. All divisional efforts were focused on the implementation of the Current Agency Accounting System upgrade thereby causing delays in projected enhancements to Accounts Receivable. Divisional resources will also focus efforts on the implementation of the New Claims Processing Systems for financial systems and data warehouse. The areas of greatest challenge are heavily entrenched in manual processes. Among these manual processes is Program Integrity's notification of recipient excess benefits. An automation project is in early development that will allow for automatic notifications and automatic retrieval of information needed to establish the receivable. Therefore, we will continue to work with the Information Management Division to implement those

enhancements we are able to do amidst projects with a higher priority. Thus expected Fiscal AR automation will be completed by September 30, 2018.

Fiscal AR is committed to improving the accounts receivable collection process and reducing the backlog of receivables. Therefore, with management approval, Fiscal AR will temporarily augment resources to effectively right-size the workload which will directly impact the reduction of the backlog and improve the timeliness in collection efforts. Increase resources are expected to be in place by June 30, 2018.

Responsible Persons:

- Karen Stephenson, Controller, DMAS Fiscal and Purchases Division

Estimated Implementation Date: December 31, 2018

Create Policies and Procedures to Ensure Compliance with Statement of Economic Interest Requirements (issued as MP#3)

Condition

Medical Assistance Services did not ensure the employees it designated as occupying a position of trust completed the required Statement of Economic Interest form. Specifically, six employees designated as required filers did not file in accordance with the Code of Virginia. Each of the six employees were either hired or transferred into positions of trust, requiring them to complete a Statement of Economic Interest form upon assuming the position. Five additional employees designated as required filers did not complete the required Statement of Economic Interest training within the required timeframe.

Recommendation

The Human Resources Division should create, implement, and maintain written policies and procedures to meet Code of Virginia requirements for the Statement of Economic Interest. These policies should incorporate guidance issued by the Commonwealth's Ethics Council. Additionally, as required by the Code of Virginia, the Human Resources Division should monitor all employees designated in a position of trust to ensure they complete the required Statement of Economic Interest training once within each consecutive period of two calendar years and maintain a record of such attendance.

Corrective Action Plan:

The Human Resources Division (HR) plans to take the following corrective actions:

1. Contact VA Ethics Council for updated guidance on system functionality since currently the Disclosure System cannot accept transfers within the Agency. Unless the system is unlocked, employees transferring to positions requiring completion of the SOEI, the coordinator cannot add them and initiate emails for completion of the Statement of Economic Interest forms. Estimated completion date: January 24, 2018.

2. Request from the Ethics Council and updated Users' Guide explaining the functionality of the system. Estimated completion date: January 8, 2018 [The Ethics Council was unable to provide updated Users Guide. HR will follow-up with new Ethics Council Coordinator.]

3. Write internal procedures for DMAS.

The following controls have been implemented:

1. Requests to Fill documents include a check off box for Statements of Economic Interest to ensure positions are added to the list to be added to the Disclosure System.
2. HR staff reviews all positions when staffing changes are announced. Employment Manager and HR Analysts notify the HR Director when required positions are filled.
3. HR Director receives notification from the Operations Manager of the new staff member's personal email address since DMAS email addresses are not set until an employee arrives and the Disclosure System cannot operate without an email address.

Responsible Persons:

- Kathleen Guinan, DMAS Human Resources Director, Human Resources Division

Estimated Implementation Date: March 31, 2018

COMMONWEALTH of VIRGINIA

DEPARTMENT OF SOCIAL SERVICES

Office of the Commissioner

Margaret Ross Schultze
COMMISSIONER

January 12, 2018

M. Martha Mavredes
Auditor of Public Accounts
101 North 14th Street
Richmond, VA 23219

Dear Ms. Mavredes:

The Virginia Department of Social Services concurs with the audit findings included in the 2017 review by the Auditor of Public Accounts.

Should you require additional information, please do not hesitate to contact Michael L. Gump, Chief Financial Officer, by email at michael.gump@dss.virginia.gov or by telephone at (804) 726-7223.

Sincerely,

Margaret Ross Schultze

801 East Main Street • Richmond, VA 23219-2901
www.dss.virginia.gov • 804-726-7011 • TTY Dial 711

AGENCY OFFICIALS

As of June 30, 2017

William A. Hazel, Jr., Secretary of Health and Human Resources

Department of Behavioral Health and Developmental Services

Jack Barber, M.D. – Interim Commissioner

Department of Health

Marissa Levine, M.D., MPH, FAAFP– Commissioner

Department of Medical Assistance Services

Cynthia B. Jones – Director

Department of Social Services

Margaret R. Schultze – Commissioner