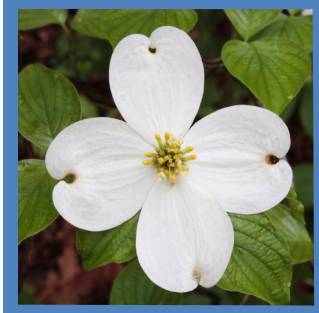


AGENICES OF THE SECRETARY OF HEALTH AND HUMAN RESOURCES

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2016

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

AUDIT SUMMARY

This report summarizes our fiscal year 2016 audit results for the following four agencies under the Secretary of Health and Human Resources. Collectively these four agencies spent $13 billion or 96 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 Accounting and Reporting System, Cardinal, each agency's accounting records, and other financial information reported to the Department of Accounts;

- thirty-four internal control and compliance findings requiring management's attention. Of these findings, two findings are considered to be material weaknesses and fifteen findings were repeated from the previous year;

- four Risk Alerts which represent issues that are beyond the corrective action of one individual agency and require the cooperation of others to address the risk; and

- two Comments to Management that represent issues we want to bring to the attention of management to ensure they are aware of the issue and can take action as needed.

This report is organized by agency and; therefore, Findings, Risk Alerts and Comments to Management are reported for each agency. Those findings that report on issues that were not resolved from our previous audit are designated with "REPEAT" at the end of their title. Additionally, the severity classification for each internal control and compliance finding is indicated for each finding. All findings are classified as either a material weakness, significant deficiency, or deficiency.

–TABLE OF CONTENTS–

What is a Risk Alert?

During the course of our audit, we encountered issues that are beyond the corrective action of DBHDS management alone and require the action and cooperation of management and the Commonwealth's Cardinal Implementation Team or the General Assembly and the Administration. The following issues represent such a risk to DBHDS and the Commonwealth.

Risk Alert - Properly Plan for CIPPS Replacement

The Department of Behavioral Health and Developmental Services (DBHDS) has several challenges to address while preparing for the Cardinal Payroll implementation, the system that will replace the Commonwealth's current payroll system, CIPPS, resulting in an increased risk that DBHDS may not be able to interface Kronos upon Cardinal Payroll's implementation. Although Cardinal Payroll is not scheduled to go-live until April of 2018, critical work by the Cardinal Payroll project team and all agencies that use CIPPS is currently underway.

Currently, DBHDS uses Kronos software for time and leave accounting, specifically its clocking functionality, which is critical for employees working in the hospital and training center environments. Kronos currently interfaces time and leave accounting data with CIPPS. Because DBHDS is running an older version of Kronos, vendor support for this version ended June 2015. Although DBHDS extended support until June 2016, they currently have no vendor support and no valid contract exists to obtain an extension. If Kronos fails, DBHDS will not be able to fix the system resulting in DBHDS having to revert to manual processes to be able to pay hospital and training center employees.

Cardinal Payroll does not contain the functionality DBHDS requires and uses within Kronos. Therefore, DBHDS plans to continue using Kronos and interface it with Cardinal Payroll. DBHDS is attempting to obtain approval for a sole source emergency procurement from the Virginia Information Technologies Agency (VITA) to upgrade Kronos; however, DBHDS has not yet determined the system requirements necessary for the upgrade. Developing requirements, procurement, design, and implementation for this type of upgrade takes on average one year; however, DBHDS may be underestimating the time and effort this process will take. Since DBHDS has no choice but to upgrade Kronos or develop another time and leave accounting process before they can create the interface to Cardinal Payroll because Kronos is unsupported, DBHDS is already facing timing constraints and ultimately may have to revert to manual processing to pay hospital and training center employees.

These challenges are of particular concern given DBHDS' similar experience with the replacement of CARS with Cardinal Financials. In preparing for the Cardinal Financials implementation, DBHDS decided to continue with its current financial management system (FMS) and interface it with Cardinal Financials. To accomplish this, DBHDS needed to first build and replace

three servers that were running on outdated software that could not support the FMS upgrade, then upgrade FMS because it was running on unsupported, end-of-life database software, and finally build an interface between FMS and Cardinal Financials. DBHDS did not complete the server build and replacement and perform the FMS upgrade until late in calendar year 2015. They could not design the interface with Cardinal Financials until this upgrade was complete. DBHDS completed the interface just in time to go live with Cardinal Financials.

The timing of implementation and lingering difficulties with the interface have caused considerable difficulties within the Central Office in completing reconciliations and processing federal transactions. It has stretched already limited resources to the point that internal controls and processes are negatively impacted. Procurement difficulties contributed to the timing issues.

To ensure a successful Cardinal Payroll implementation, DBHDS should properly plan the timing and procurement of the hardware and software needed to upgrade Kronos and interface it with Cardinal Payroll. This includes working with VITA and the Cardinal Payroll implementation team to make the appropriate decisions and take the appropriate steps to ensure that they have a system that can satisfy their time and leave accounting needs, but can also timely interface with Cardinal Payroll upon implementation.

Risk Alert – Continue to Comply with the DOJ Settlement Agreement – REPEAT

In January of 2012, the Commonwealth of Virginia and the United States Department of Justice (DOJ) reached a settlement agreement to resolve a DOJ investigation of the Commonwealth's training centers and community programs under the jurisdiction of DBHDS. This settlement agreement also addressed the Commonwealth's compliance with both the Americans with Disabilities Act and the U.S. Supreme Court Olmstead ruling requiring individuals be served in the most integrated settings appropriate to meet their needs. The major highlights of the settlement include the expansion of community-based services through waiver slots; strengthened quality and risk management systems for community services; and the transitioning of affected individuals from the training centers to new homes in the community.

The Commonwealth continues to work with DOJ and an independent reviewer to meet the terms of the settlement agreement. DBHDS plans to close four out of its five training centers by 2020. Southside Virginia Training Center and Northern Virginia Training Center closed in May 2014 and March 2016, respectively. Southwest Virginia Training Center and Central Virginia Training Center will close June 2018 and June 2020, respectively. There is a risk of future non-compliance if DBHDS does not receive adequate funding at the appropriate time for the transition programs and a stoppage of services results. This is of particular concern since the Commonwealth experienced a budget shortfall at the end of fiscal year 2016, which will result in statewide budget cuts. These cuts have the potential to impact compliance if funding is removed or reduced for any of the items below. Loss or reduction in funding could extend the time that it takes for DBHDS to implement programs, move individuals into the community, and reach the other requirements of the DOJ settlement agreement. Specifically, funds are needed:

- to address critical and ongoing one-time requirements to continue building community capacity as well as remain compliant with other aspects of the settlement agreement;

- to support facility transition waiver slots to enable DBHDS to continue moving individuals out of the training centers and into community based programs as well as additional community living (CL), family and individual support (FIS), and building independence (BI) waiver slots to help reduce the growing waiting list for services; and

- to support individuals in community based programs with housing, transportation, and other services.

We continue to encourage DBHDS, the General Assembly, and the Administration to work together to ensure that DBHDS has the funds and support it needs to continue to comply with the settlement agreement and provide services to individuals in the appropriate setting.

Why the APA Audits Contractual Commitments

DBHDS contractual commitments are material to the Commonwealth's CAFR. Incorrect reporting of contractual commitments could cause a material misstatement in the CAFR disclosures. We reviewed the Contractual Commitments Attachment submitted by DBHDS to the Department of Accounts (Accounts) and determined the adjustments needed to properly reflect the commitments in the CAFR disclosures.

Improve Controls over Financial Reporting

Severity: Material Weakness

Condition

DBHDS does not have an adequate process to compile contractual commitment information for submission to Accounts for inclusion in the Commonwealth's Comprehensive Annual Financial Report. As a result, DBHDS overstated construction obligations by approximately $38.7 million and understated other contractual obligations by approximately $11.2 million. Because of the magnitude of this misstatement, we consider this to be a material weakness.

Criteria

The Comptroller's Directive establishes compliance guidelines and addresses financial reporting requirements for state agencies to provide information to Accounts for the preparation of the Comprehensive Annual Financial Report as required by the Code of Virginia. Accounts requires DBHDS to submit information as prescribed in the Comptroller's Directives and individuals preparing and reviewing the submissions are required to certify the accuracy of the information provided to Accounts.

Consequence

Inaccurate compilation of contractual commitment amounts submitted to Accounts could materially misstate the commitments disclosure in the Comprehensive Annual Financial Report.

Cause

DBHDS' Budget and Financial Reporting Manager did not adequately communicate with the Architecture and Engineering and Procurement Departments to determine the contractual obligations at year-end. The Budget and Financial Reporting Manager provided the Architecture and Engineering Department prior year contract amounts to update for the construction commitments; however, did not explain the significance of the requested updates. The Deputy Director of Architecture and Engineering updated the construction commitments with current year information without validating prior year contract amounts. In addition, the Budget and Financial Reporting Manager did not communicate with the Procurement Department to determine whether there were any other contractual commitments; and therefore, did not report any in the financial information submitted to Accounts. Lastly, the Director of Budget and Financial Reporting did not identify these errors upon review of the submission and Internal Audit did not perform their usual review of the submission to ensure it was accurate and reasonable.

Recommendation

DBHDS' Office of Budget and Financial Reporting should develop and implement policies and procedures for compiling each piece of financial information, such as commitments, submitted to Accounts. Budget and Financial Reporting should involve the appropriate departments when developing these procedures to ensure that all aspects of the compilation process are documented. They should ensure the procedures over these areas provide personnel sufficient information on the purpose and importance of the information requested and direction regarding the support needed to prepare the submission, as well as adequate controls to prevent or detect and correct mistakes. DBHDS should supplement this by increasing overall review of submissions to ensure they are reasonable and accurate.

Why the APA Audits Information Systems Security

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 database security, oversight of sensitive systems, and systems access was adequate, we compared the practices of DBHDS to those required by the Commonwealth's Information Security Standard.

Continue to Improve IT Governance – REPEAT

Severity: Significant Deficiency

Condition

DBHDS is not protecting sensitive Commonwealth data in accordance with the Commonwealth's standards and has an insufficient governance structure to manage its information security program. DBHDS has a decentralized information technology (IT) environment that allows the Central Office and 15 separate facilities to manage and maintain sensitive systems independently.

Due to the decentralized IT environment, DBHDS still has over 240 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, OneMind. DBHDS intends OneMind to be an enterprise solution; however, only three facilities are using it, and there is no timetable or plan to implement OneMind at the other facilities because DBHDS lacks the IT resources and funding.

DBHDS has made progress and reduced the total number of sensitive systems from 437 to 240 sensitive systems since our last review. However, this significant number of sensitive systems requires extensive IT resources to ensure compliance with the agency's enterprise security program and the Commonwealth's Information Security Standard, SEC 501-09 (Security Standard). Managing and maintaining over 240 sensitive systems, while significantly less than 437, is still not feasible with DBHDS' current resource levels, and while DBHDS has made progress to consolidate, decommission, and upgrade applications, they should continue to consolidate the disparate systems performing similar business functions across the entire agency.

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
- Software baseline configurations
- Database Security

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 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 any IT governance changes and rectify the control deficiencies. Implementing these recommendations will help ensure the confidentiality, integrity, and availability of DBHDS' sensitive data.

Continue to Upgrade Unsupported Technology – REPEAT

Severity: Significant Deficiency

Condition

DBHDS is not protecting sensitive data by using end-of-life or end-of-support technology for sensitive systems. DBHDS has worked to upgrade, consolidate, and decommission the end-of-life systems that contain HIPAA data, mission-critical financial data, and Personal Health Information (PHI) data. The applications using unsupported technology contain sensitive and mission critical data, which increases the risk a malicious attacker can exploit a known vulnerability. We identified and communicated the control weakness to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

Criteria

The Security Standard, Section 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 or end-of-support technology, DBHDS can no longer receive and apply security patches for known vulnerabilities, which increases the risk a malicious attacker will exploit these vulnerabilities leading to a data breach. Additionally, vendors do not offer operational and technical support for end-of-life or end-of-support technology, which effects data availability by increasing the difficulty of restoring system functionality if a technical failure occurs.

Cause

DBHDS is not performing certain tasks to meet the requirements in the Security Standard and has a decentralized IT environment.

Recommendation

DBHDS should continue to prioritize the upgrade, consolidation, or decommission of all end-of-life or end-of-support technology. DBHDS should evaluate the current IT resource level and consider hiring additional resources to expedite the process. Also, DBHDS should implement mitigating controls for all sensitive systems that contain sensitive data. Doing this will reduce the risk to confidentiality, integrity, and availability of sensitive Commonwealth data.

Develop Baseline Configurations for Information Systems – REPEAT

Severity: Significant Deficiency

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 240 sensitive systems, with some containing HIPAA data, social security numbers, and PHI data.

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
  (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 240 sensitive systems, with some containing HIPAA data, social security numbers, and PHI data and by not having baseline configurations, it increases the risk 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 has procedures documenting application security requirements, but they do not contain minimum baseline configurations. The agency also lacks the necessary resources to properly monitor and maintain baseline configurations for their sensitive systems.

Recommendation

DBHDS should establish and document security baseline configurations for their sensitive information systems to meet the requirements in the Security Standard. DBHDS should evaluate its IT resource levels to make sure the resources necessary are available to ensure the security baseline configurations are, at a minimum, in place on all sensitive systems. Doing this will help ensure the confidentiality, integrity, and availability of the agency's sensitive data.

Improve SQL Database Security

Severity: Significant Deficiency

Condition

DBHDS operates its database that stores its financial activity without implementing the minimum controls in accordance with internal policy, the Security Standard, and industry best practices. We communicated seven areas of weakness to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under Section 2.2-3705.2 of the Code of Virginia, due to their sensitivity and description of security controls.

Criteria

The Security Standard requires implementing specific controls to reduce unnecessary risk to data confidentiality, integrity, and availability.

Consequence

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

Cause

DBHDS upgraded the application and had the vendor perform the majority of the upgrade. The vendor installed the database with many of the default settings and configurations, and DBHDS lacks the technical resources to properly secure the database and align settings and configurations with Security Standard requirements and best practices.

Recommendation

DBHDS should develop policies and procedures specific to the risks present in its database environment and develop a process to ensure configurations and controls align with the Security Standard and industry best practices. Management should review and approve all newly created policies and procedures and dedicate the necessary resources to remedy all the deficiencies that exist in the database environment in a timely and proactive manner. Management should also evaluate their technical resource level and determine if there are sufficient resources to manage the agency's database environment. If necessary, management should hire more resources or prioritize its corrective action implementation to address the highest risk areas. Doing this will help maintain the confidentiality, availability, and integrity of DBHDS data and meet the requirements in the Security Standard.

Improve Access Controls over Financial Management System – REPEAT

Severity: Significant Deficiency

Condition

DBHDS did not adequately plan for the upgrade of its Financial Management System (FMS) and subsequent interface to the Commonwealth's new accounting system (Cardinal) to allow the necessary IT resources and time to establish proper policies, procedures, and controls over system access to FMS. DBHDS has not documented what the critical ledgers and roles are in the newest FMS version and did not identify which roles, when combined and assigned to one person, result in a separation of duties issue. In addition, DBHDS does not have controls in place for times when it is necessary to assign conflicting roles to an individual to ensure that users with this access are not improperly using the access. DBHDS did not update the form used to request, change, and delete access to FMS to agree with the design of the upgraded system. DBHDS does not have a process to monitor access annually for all regions and facilities.

As a result of the above inadequacies, we found the following issues with employee access to FMS.

- Seven out of 21 (33 percent) users tested had access to FMS that did not agree with the approved access on the request form.

- Eight out of eight (100 percent) users tested with potential conflicting roles did have separation of duties issues.

- Five out of 21 (24 percent) users tested had FMS access that was not consistent with the employee's job duties.

- Two out of ten (20 percent) terminated users tested had their access removed untimely (not within five business days). Removal for these individuals took between 8 and 71 days.

- Ten out of 32 (31 percent) users tested had access forms that were not completed properly due to an inaccurate approval date, no HIPAA Confidentially Statement Signature, or handwritten changes to the form.

Criteria

The Security Standard, Section AC-2-COV 2 a, requires a documented request to establish an account. The Security Standard, Section AC-2-COV 2 e and f, require prompt notification and removal of access for transferred or terminated users. The Security Standard, Section AC-5 a-c, requires that system access be defined and assigned to support separation of duties. The Security Standard, Section AC-6, requires granting access based on the principle of least privilege and part seven in that section requires the performance of an annual review of access to validate that the need still exists.

Consequence

Not ensuring that system users have and retain appropriate access to FMS increases the risk of unauthorized individuals inappropriately entering or approving transactions and could affect the integrity of DBHDS transactions in the FMS and Cardinal systems.

Cause

DBHDS did not update access forms, document policies, identify critical roles, and properly assign and remove access because of a lack of planning for the FMS upgrade and a lack of IT resources. After upgrading FMS, the IT resources available focused on developing the interface with Cardinal and then the implementation of Cardinal. In addition, DBHDS has not trained its facility managers and regional system administrators on how to assign, change, and remove user access.

Recommendation

DBHDS management should establish and implement proper policies, procedures, and controls over access to FMS. DBHDS should document the critical ledgers and roles and identify those that when combined can result in separation of duties issues. When individuals must have conflicting roles, DBHDS should establish controls to detect any inappropriate or fraudulent transactions by those individuals. DBHDS should update the access form to reflect the upgraded system and train facility managers and regional system administrators on completing the access forms. Finally, DBHDS should ensure access is reviewed annually to identify unnecessary access due to terminations or changes in position.

Improve Internal Controls Surrounding Sensitive Documents

Severity: Significant Deficiency

Condition

DBHDS did not always ensure that unencrypted sensitive documentation is not transmitted using email communication. The DBHDS Central Office uses the Payroll Service Bureau (PSB) for their payroll processes. Since PSB's implementation, the Central Office has emailed scanned copies of payroll reports to PSB on a regular basis without encrypting the information being sent. In addition, during our audit, DBHDS employees emailed the Auditor of Public Accounts unencrypted emails containing sensitive information nine times even after being repeatedly reminded not to email these types of items. The payroll reports and the information emailed to the auditors included sensitive information, which included the combination of employee name, employee identification number, employee birthdate, and salaries.

Criteria

The Security Standard, Section SC-8-COV, requires the use of data protection mechanisms for the transmission of all email and attached data that is sensitive. The Security Standard requires the use of encryption or digital signatures for the transmission of email and attached data that is sensitive relative to integrity and confidentiality.

The VITA defines sensitive data as "any data of which the compromise with respect to confidentiality, integrity, and/or availability could adversely affect COV interests, the conduct of Agency programs, or the privacy to which individuals are entitled." Examples of sensitive data include but are not limited to: Personally Identifiable Information, including information that describes, locates or indexes anything about an individual including financial transactions, social security numbers, medical history, ancestry, religion, political ideology, criminal or employment record and photographs.

Consequence

Email is the quickest and easiest way to communicate. However, without sufficient safeguards over sensitive data in email communications, it can leave DBHDS in violation of privacy requirements, industry regulations, and government mandates. Not encrypting the information also increases the risk that someone can intercept the message thus compromising DBHDS employee or patient information.

Cause

Some DBHDS employees did not have an accurate understanding of the encryption process required when transmitting sensitive data using email communication. DBHDS has been operating under the impression that as long as the emails were not leaving the state's network, then there was

no need to encrypt the emails. Given the department-wide misunderstanding of the requirement, it is probable that DBHDS employees have emailed other sensitive information over the years.

Recommendation

DBHDS should ensure all employees accurately understand the Security Standards. All employees should use secure methods to send sensitive information, which include but are not limited to encrypted emails, faxes, and secure file sharing sites. These methods should be used when sending anyone, including PSB and the auditors, sensitive documents.

Why the APA Audits an Agency's Controls over their Information in the *my*VRS Navigator System

The *my*VRS Navigator system is used to calculate total pension liabilities for the Commonwealth. Individual agencies are responsible for updating the records within *my*VRS Navigator 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 *myVRS* Navigator – REPEAT
Severity: Significant Deficiency

Condition

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

- Eleven of thirteen facilities tested did not have adequately documented policies and procedures to reconcile their payroll and human resource systems to the *my*VRS Navigator system;

- Four of six facilities tested did not perform or could not provide evidence that they performed all required parts of the monthly reconciliations between the Commonwealth's personnel system, PMIS, and *my*VRS Navigator before certifying contribution snapshots; and

- One of eighteen individuals tested had improper *my*VRS Navigator access, which caused a segregation of duties issue.

Criteria

Accounts Payroll Bulletin Volume 2013-02 states that agencies must certify the Contributions Snapshot by the tenth of the following month, as it becomes the official basis for VRS billing amounts once certified. In addition, it is best practice to create and document formal policies and procedures to ensure that reconciliations are performed between *my*VRS Navigator and the systems of record for payroll and human resources and to ensure that *my*VRS Navigator system access is both role based and centered on least privileges.

Consequence

Untimely certification at the agency level impacts the ability of Accounts to process Inter-agency Transfers for any differences between the amounts confirmed in *my*VRS Navigator and the retirement contributions actually withheld and paid for all agencies across the Commonwealth. Inadequate written policies and procedures at DBHDS facilities provides insufficient guidance for employees to perform the reconciliations necessary to perform these certifications. Inappropriate access to the *my*VRS Navigator system, through improper segregation of duties and untimely removal of system access, creates the potential for inaccurate information to appear in the VRS system data that ultimately determines pension liability calculations for the entire Commonwealth. The VRS actuary uses the information in *my*VRS Navigator to calculate the Commonwealth's pension liabilities and inaccurate data could lead to a misstatement in the Commonwealth's financial statements.

Cause

Staffing shortages, turnover, a lack of understanding, and inadequate oversight all contributed to the lack of documented policies and procedures as well as the improper performance of the reconciliations. The improper segregations of duties access observed involved inappropriately setting up access when initially implementing *my*VRS Navigator.

Recommendation

Management should formally document policies and procedures necessary to perform the monthly reconciliations between the payroll, human resource, and *my*VRS Navigator systems at all facilities and maintain evidence for the performance of those procedures. Management should implement adequate controls and procedures at the facilities that consider staffing and other priorities to ensure monthly reconciliations are performed prior to Snapshot certification. Finally, management should ensure appropriate *my*VRS Navigator system access exists at all facilities including issuance of access based on least privileges.

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 Commonwealth Accounting Policies and Procedures (CAPP) Manual, resulting in the findings below.

Improve Controls over Payroll – REPEAT

Severity: Significant Deficiency

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:

- Six out of 52 (12 percent) Kronos users tested did not complete the KRONOS access form timely and 15 out of 52 (29 percent) Kronos users tested had access to KRONOS that did not agree to the approved access on the request form.

- Three out of 104 (three percent) salaried employees tested did not have the most recent PAW (Personnel Action Worksheet) on file, five out of 104 (five percent) salaried employees tested did not have a PAW that contained all required signatures for approval, and two out of 104 (two percent) salaried employees tested did not have the most current employee evaluation completed and or signed.

- Four out of 54 (seven percent) terminated employees tested had the termination date entered in Kronos incorrectly and one out of 54 (two percent) terminated employees tested had their leave payout calculated incorrectly. In addition, one facility did not maintain adequate payroll records to support terminations.

- Two out of 48 (four percent) new hires tested did not have a complete PAW and five out of 48 (ten percent) new hires tested did not have a PAW in the payroll file.

- One facility did not remove dual PMIS and CIPPS access for a terminated employee until approximately nine weeks after their termination.

- One facility had a part-time employee that worked more than 1,500 Hours.

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 CIPPS.

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.

Chapter 665 §4-7.01 g. of the 2015 Virginia Acts of Assembly states that "State employees in the legislative, judicial, and executive branches of government, the independent agencies of the Commonwealth, or an agency administering their own health plan, who are not eligible for benefits under the health care plan established and administered by the Department of Human Resource Management ("DHRM") pursuant to Va. Code § 2.2-2818, may not work more than 29 hours per week on average over a twelve month period."

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 employees increases the risk of unauthorized individuals inappropriately entering or approving transactions and could compromise sensitive employee information. Not complying with Chapter 665 of the 2015 Virginia Acts of Assembly subjects DBHDS to potential financial penalties for violation of the Federal Affordable Health Care Act by allowing workers to work over the threshold and not receive healthcare benefits.

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 facility 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 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 and have an adequate process for monitoring employees' hours to ensure no one exceeds the allowable threshold. Lastly, management for all facilities should remove all access in a timely manner for employees that are terminated or no longer need access.

Improve Internal Controls Surrounding At-Will Employees

Severity: Deficiency

Condition

DBHDS' Human Resources Department (Human Resources) does not ensure that they receive and maintain written certification for their at-will employee establishing that the employee has not exceeded their leave limit during the allotted time period. In addition, Human Resources did not provide a letter certifying that leave balances were accurate when an at-will employee transferred to a new state agency. At-will employees are individuals appointed by the Governor of Virginia, such as Cabinet members or agency heads.

Criteria

The Commonwealth's Executive Leave Policy requires all at-will employees to certify, in writing, that they have not exceeded their established leave limit during the allotted time period. The employees should maintain a leave calendar to attach to the certification letter. The agency's Human Resource Office should maintain the certification letter and make it available for review by the Auditor of Public Accounts.

In addition, if an at-will employee transfers to a different at-will position in another agency and they have leave balances, the balance transfers. The transferring agency must prepare a letter certifying that the balance is accurate and should include this letter with official transfer documents.

Consequence

Without maintaining the leave certification letter, DBHDS cannot provide assurance that their at-will employees complied with the provisions set forth within the Executive Leave Policy.

Cause

The Human Resources Department was unaware of the requirement and did not require at-will employees to submit their leave calendar and certification letter.

Recommendation

Human Resources should ensure that all at-will employees are made aware of the Commonwealth's Executive Leave Policy. At-will employees should ensure that they complete and

submit a written certification establishing that they did not exceed their leave limits during the allotted time period. At-will employees should submit the certification along with their leave calendar to Human Resources annually. Human Resources should review this documentation for reasonableness to ensure that the employees did not exceed their leave balances. Lastly, when at-will employees transfer to another agency Human Resources should ensure that they prepare a letter certifying that the leave balances transferring are accurate and include this letter with official transfer documents.

Why the APA Audits Compliance with the Statement of Economic Interest

DBHDS has designated 61 people in a position of trust across the state. The Code of Virginia requires all individuals in a position of trust to submit Statement of Economic Interest Disclosure Forms and complete related training. To determine if DBHDS complies with the Code of Virginia, we compared the practices of DBHDS to those required by the Code of Virginia.

Comply with the *Code of Virginia* Economic Interest Requirements – REPEAT

Severity: Significant Deficiency

Condition

DBHDS did not ensure all employees designated to be holding a "positon of trust" are submitting the Statement of Economic Interest (SOEI) forms timely, nor completing the required Statement of Economic Interest training every two years. In addition, DBHDS does not maintain a record of training attendance as required. Two out of seven employees in a position of trust tested did not submit their SOEI form timely, and five out of seven employees did not attend the required training.

Criteria

Pursuant to Sections 2.2-3114 and 3128 through 3131, of the Code of Virginia, employees designated to be in a "position of trust" must file a SOEI form set forth in Section 2.2-3117 semiannually by December 15 for the preceding six-month period complete through the last day of October and by June 15 for the preceding six-month period complete through the last day of April. Additionally, filers must complete orientation training about the Conflict of Interest Act that will help them recognize potential conflicts of interest. The filers must complete this orientation within two months of hire/appointment and at least once during each consecutive period of two calendar years. The Office of the Attorney General offers and approves the training to instruct agencies within the Commonwealth. The training educates employees on how to recognize and avoid a conflict, or the appearance of a conflict, of interest and the measures to remedy the conflict. DBHDS must keep a record of attendance for five years including the specific attendees, each attendee's job title, and dates of their attendance.

Consequence

DBHDS could be susceptible to conflicts of interest that would impair or appear to impair the objectivity of certain programmatic or fiscal decisions made by employees in positions designated as "position of trust." By not requiring employees to complete the training and keeping record of the attendance for the training, DBHDS may not be able to hold its employees accountable for knowing how to recognize a conflict of interest and how to resolve it.

Cause

The Statement of Economic Interest Coordinator is responsible for maintaining and submitting the list of individuals who are required to file a SOEI form. However, due to turnover in this position, DBHDS does not monitor and track submissions to ensure timeliness. In addition, management did not issue agency-wide guidance that communicated the requirements of when employees should complete the statement of economic interest training and that the Coordinator should maintain record of attendance for the training. The individuals that did not attend the required training were not aware of the requirement or they were not reminded of the requirement. DBHDS did not implement additional processes or controls to correct this same problem identified in the prior audit.

Recommendation

DBHDS should ensure all employees in a position of trust complete the required SOEI form timely, ensure filers complete training once within each consecutive period of two calendar years, and maintain a record of such attendance for five years.

Why the APA Audits Fixed Assets Management

DBHDS has 15 individual locations throughout the Commonwealth. As part of its plan to comply with the DOJ settlement, DBHDS plans to close two more facilities by the end of fiscal year 2020. Because of the large number of fixed assets associated with multiple locations, DBHDS management must take necessary precautions to account for all fixed assets properly. To determine if fixed assets are accounted for properly, we compared the practices of DBHDS to those required by the CAPP Manual.

Improve Controls over Intangible Assets – REPEAT

Severity: Deficiency

Condition

DBHDS Fiscal Services does not have adequate policies and procedures to identify and capitalize intangible assets. DBHDS created policies during fiscal year 2016; however, these policies and procedures lack the method, the timing, and the system DBHDS Central Office plans to use to track and report construction-in-progress (CIP) and capitalizable intangibles. In addition, the policies do not address software licenses. We identified this issue in the prior year's audit, and DBHDS has not made notable progress in correcting this deficiency.

DBHDS lacks controls and procedures to ensure they properly identify, track, record, and report all intangibles to Accounts. As a result, they are improperly recording intangible assets and CIP in the Commonwealth's Fixed Asset Accounting and Control System (FAACS) and Accounts Attachment 14. In addition, because DBHDS does not have adequate procedures to track and capitalize CIP expenses, we are unable to determine whether the amounts recorded are accurate.

- Fiscal Services did not properly account for the completion or stoppage of at least four intangible projects within CIP during fiscal year 2016 by not removing them from CIP and either capitalizing or expensing them. These four projects potentially overstate CIP by approximately $2 million.

- Fiscal Services did not record two systems development projects, Transition Support Tracking and FMS Upgrade/Cardinal Data Exchange, in CIP during the fiscal year. The Transition Support Tracking project, with a budget of $538,000, began in fiscal year 2014 and was cancelled in fiscal year 2016; however, Fiscal Services never recorded the expenses in CIP. The FMS Upgrade/Cardinal Data Exchange, with a budget of $783,000, began in fiscal year 2015 and was completed in fiscal year 2016, and Fiscal Services did not record the project expenses in CIP nor did they record it as a complete intangible asset.

- Information Technology has identified new technology projects potentially meeting the intangible assets requirements and a multi-year license agreement, but did not communicate this information to Fiscal Services. Therefore, Fiscal Services did not include the projects or license in CIP or capitalize them.

Criteria

CAPP Manual Topic 30325 - Software and Other Intangible Assets states, "During the development stage, evaluate the expenditures to determine whether capitalization appears appropriate. Record the applicable capitalizable expenditures as Construction in Progress. To ensure appropriate financial control of Construction in Progress, project numbers should be assigned to identify related expenditures." CAPP Manual Topic 30325 also indicates that software licenses

should be evaluated to determine if they should be capitalized as an intangible asset. Lastly, CAPP Manual Topic 30325 indicates that the assets are to be recorded in a timely manner.

Consequence

Improperly recording intangible CIP in FMS, FAACS, and Attachment 14 could misstate the financial reporting of current CIP and future intangible capitalization in the Commonwealth's Comprehensive Annual Financial Report. Because DBHDS did not implement corrective action since last year and did not provided intangible asset documentation to the auditors for review, we are unable to determine the extent of these misstatements and misclassifications.

Cause

Although Fiscal Services created policies and procedures during the fiscal year, the policies did not include all elements necessary, and Fiscal Services did not convey the policies to all departments and facilities that play an integral role in identifying, tracking, and capitalizing the intangible assets. In addition, there is a severe lack of communication between Fiscal Services and Information Technology related to intangibles. Information Technology is not aware of the policies or procedures; and therefore, does not notify Fiscal Services when projects are completed or stopped due to lack of funding. Furthermore, Fiscal Services does not have adequate controls to ensure that DBHDS' Financial Management System (FMS), FAACS, and Accounts attachments are accurate and consistent.

Recommendation

Fiscal Services should improve the policies and procedures related to intangibles by developing and implementing detailed policies and procedures that include the responsible party, the method, the timing, and the system DBHDS Central Office plans to use to track and report CIP and capitalizable intangibles. The procedures should specifically include a process to identify multi-year licenses for potential capitalization. The policies and procedures should also indicate date of effectiveness, approver, and date of annual reviews. Most importantly, Fiscal Services should work with Information Technology to determine the stages of a project and perform analysis or review at each stage of the project as appropriate to ensure that the project is properly capitalized or expensed at the end of the project. Finally, Fiscal Services should review each ongoing and recently completed project to ensure that project-related expenses are properly included in CIP, capitalized as an asset, or expensed.

Improve Policies and Procedures over Fixed Assets – REPEAT

Severity: Deficiency

Condition

DBHDS lacks adequately documented and approved policies and procedures for fixed assets. The policies and procedures that do exist vary between facilities and the Central Office by content,

adequacy, and existence. The areas that are not clearly documented and approved include but are not limited to:

- Fixed Assets Accounting System (FAACS)
- Disposals
- Donations
- Reconciliations
- Intangible Assets
- Sales of all asset categories
- Surplus of all asset categories
- Transfers
- Useful life assessment and reevaluation

In addition, multiple DBHDS facilities and Central Office have policies and procedures that management has not documented that they have reviewed since implementation in 2009.

Criteria

CAPP Manual Topic 20905 - CARS Reconciliation Requirements states that CAPP Manual procedures alone never eliminate the need and requirement for each agency to publish its own internal policies and procedures documents, approved in writing by agency management. The lack of complete and up-to-date internal policies and procedures (customized to reflect the agency's staffing, organization, and operating procedures) reflects inadequate internal controls.

Consequence

The lack of fixed asset policies and procedures increases the risk of inaccurate accounting of fixed assets and contributed to the issues discussed in the findings "Improve Controls over Fixed Asset Additions," "Improve Controls over Intangible Assets," and "Improve Controls over Sale of Land."

Cause

DBHDS has not allocated or prioritized the appropriate resources to ensure that such internal policies and procedures over fixed assets are present at all DBHDS facilities and Central Office.

Recommendation

Management should update, communicate, and implement policies and procedures over fixed assets at all DBHDS facilities and the Central Office. In addition, management should periodically review the policies and procedures to determine whether they need to be updated as a result of changes in accounting standards, agency systems, or other processes.

Improve Controls over Sale of Land – REPEAT

Severity: Deficiency

Condition

DBHDS still does not have adequate policies and procedures related to the sale of land. We identified an issue with recording partial land sales in the prior year. Since then, Fiscal Services developed a policy on how facilities should handle the recording of these sales. The policy is still missing a few key items, such as the responsible party, timing, revenue verification, acquisition date, evidence of management review, approval, and effective date of the policy. In addition, the policy does not appropriately identify that facilities should use and update the acreage for the property in FAACS based on the amount sold. The policy, instead, just references updating the quantity, which has caused confusion for facility staff. DBHDS facilities did properly record two partial land sales in fiscal year 2016, except for recording the wrong acquisition date for one. DBHDS has not reviewed and corrected all past partial land sales in FAACS, including determining the number of acres, resulting in several pieces of land being overstated for the disposed portions. Southeastern Virginia Training Center attempted to make one correction, but recorded the correction twice and an incorrect acquisition date, overstating assets in FAACS. Furthermore, Fiscal Services did not confirm the proceeds from the sale of land they received from Department of General Services with support for the sale price and fees.

Criteria

Both CAPP Manual Topic 30805 - Disposal Management and DBHDS FAACS Updates on Property Sales indicate at the time the disposal transaction is processed, the book value of the asset is removed from the FAACS financial reporting file. It is important for assets that are no longer under the control of the agency to be disposed in FAACS to ensure that financial statements containing capital asset information are accurate. Furthermore, agencies should periodically review the capital asset information contained in FAACS to ensure that assets that are no longer under the control of the agency have been properly disposed in FAACS. In addition, disposals should be recorded in FAACS during the fiscal year in which the change in asset status occurred. When partial property is sold, the original acquisition date should be recorded in FAACS. Finally, it is best practice to confirm the revenues received from other state agencies are accurate through support of the sale and fees.

Consequence

Not removing asset values for partial land sales and improperly recording a correction twice resulted in an overstatement of assets in FAACS.

Cause

Although Fiscal Services created policies and procedures during the fiscal year, the policies did not include all elements necessary. In addition, there is a severe lack of communication between Central Office Fixed Asset Accountants, Fiscal Services, Architecture and Engineering, and the Facilities Fixed Asset Accountants resulting in confusion and misunderstandings about the process.

Recommendation

Fiscal Services should improve the policies and procedures related to the sale of land and implement detailed policies and procedures that include the responsible party, timing, revenue verification, acquisition date, and evidence of management review, approval, and effective date of the policy. In addition, Fiscal Services should work with the facilities to determine land acreage for parcels of land that they plan to sell in the near future so that they are prepared for the process to record the disposal when it occurs. Finally, Fiscal Services should work with the facilities to correct the improperly recorded disposals identified in the fiscal year 2015 audit.

Improve Internal Controls over Fixed Asset Additions – REPEAT

Severity: Deficiency

Condition

Individual facilities within DBHDS do not have adequate policies and procedures in place to ensure fixed assets are recorded in FAACS timely. Ten out of 14 facilities and the Central Office recorded 49 percent of their fiscal year 2016 fixed asset acquisitions more than 30 days after receipt and acceptance of the asset. Southeast Virginia Training Center inappropriately recorded asset transfers received from Northern Virginia Training Center using fair market value.

In addition, DBHDS' Central Office Architecture and Engineering Services (Architecture and Engineering), does not provide the facility FAACS coordinators with detailed information to allow them to timely transfer assets from CIP to the proper depreciable capital asset category.

We identified these issues in the prior year's audit, and DBHDS has made some progress in correcting the deficiencies, with the error rate dropping from 93 percent to 49 percent, but needs to continue strengthening these processes.

Criteria

CAPP Manual Topic 30205 - Acquisition Method states, "All recordable assets, except constructed assets, should be recorded in FAACS 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 FAACS in the fiscal year the asset was acquired. Similarly, asset disposals should be posted to FAACS in the fiscal year the disposal occurred. For equipment, title is considered to pass at the date the equipment is received. Constructed assets are transferred from the construction in progress account to the related building, infrastructure, or equipment accounts when they become operational. Constructed buildings, for example, are assumed to be operational when an authorization to occupy the building is issued, regardless of whether or not final payments have been made on all the construction contracts."

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 fixed assets increases the risk that asset balances, including depreciation expense, are misstated, which can affect the facilities Medicaid reimbursements and the Commonwealth of Virginia's Comprehensive Annual Financial Report.

Cause

DBHDS does not have adequate processes to ensure timely recording of asset acquisitions in FAACS. DBHDS facilities gave various reasons for delays in asset recording. These include not recording received assets until in use, not forwarding the correct information to the FAACS coordinator timely, not understanding how the asset should be recorded, receiving incorrect Governmental Accounting Standards Board (GASB) guidance from the Internal Audit Director, having password issues with FAACS, and encountering issues and limited staffing levels during Cardinal implementation. In addition, Architecture and Engineering, in managing CIP, does not gather and communicate to facilities the detailed information needed by FAACS coordinators to timely transfer items out of CIP and record them in the appropriate capital asset categories.

Recommendation

Management should create, communicate, and implement policies and procedures over fixed asset recording 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. Facilities should plan to have personnel available to process FAACS entries timely when new systems are being implemented. 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 FAACS when they are transferred from closed facilities to other DBHDS facilities and other state agencies. Internal Audit should ensure that the guidance provided follows the most recent GASB pronouncements as well as the CAPP Manual. In addition, Architecture and Engineering should obtain adequate information from contractors and provide this to the facilities' FAACS coordinators to allow timely recording of assets transferred out of CIP.

Why the APA Audits Inventory

Health's inventory primarily consists of pharmaceuticals valued at approximately $23 million in fiscal year 2016. This inventory is material to the Commonwealth's financial statements and incorrect reporting of inventory could cause material misstatement of total inventories reported. We reviewed the Inventory Attachment submitted by Health to the Department of Accounts (Accounts); observed year-end inventory counts performed by Health's central pharmacy; and performed test counts and recalculations of inventory totals.

Improve Inventory Valuation Procedures

Severity: Material Weakness

Condition

Health does not have procedures to ensure pharmacy inventory is properly valued. The pharmacy relies on a third party vendor to provide cost information for valuation of the year-end inventory, but does not have any formal policies and procedures to ensure the cost information used to value the inventory is accurate. For example, Health does not obtain an audit report of the third party vendor to gain assurance over the controls in place nor do they do they perform any other procedures to confirm costs used in the year-end inventory calculation.

Criteria

Health is responsible for determining the internal controls over inventory are adequate to ensure financial information reported to Accounts is accurate and fairly stated. Health year-end inventory is material to the Commonwealth's financial statements.

Consequence

Health overstated their year-end inventory amount reported to Accounts by $577,138. The third party vendor incorrectly reported the price of one drug, doubling the cost for that drug, and this was not detected by Health before the information was sent to Accounts. As a result, Health had to resubmit the attachment to correct the errors, resulting in inefficiencies. In addition, there were four other drugs where the year-end value did not agree to recent invoices, although these differences were immaterial.

Cause

The Pharmacy Director relies on individual item prices input by the third party vendor into the inventory management system and performs no review of uploaded prices. While the Pharmacy

Director prepares a reconciliation of the top ten drug items to ensure inventory counts are accurate, there is no formal reconciliation or review of cost information.

Recommendation

Health and pharmacy management should develop policies and procedures over inventory valuation. Consideration should be given to obtaining assurances from the third party vendor as well as additional procedures that pharmacy staff should perform as part of their inventory process. Procedures could include a review of year-end costs, particularly for drugs where there are significant quantities or where the cost is significant.

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 Information Security Standards in the areas of web application security, oversight of sensitive systems, and information system access.

Improve Timely Removal of Critical Access – REPEAT

Severity: Significant Deficiency

Condition

Individual department supervisors are not completing and sending employee separation forms (HR-14 forms) to the Office of Human Resources (OHR) in a timely manner. As a result, Health is not able to remove access for terminated employees from their internal systems timely. Access was removed between 11 and 29 days late for three out of 25 (12 percent) employees reviewed with COV and WEBVISION access.

Criteria

Section AC-2 of the Commonwealth's Security Standard requires "notifying account managers…when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes." In addition, the Security Standard states that each agency shall "promptly remove access when no longer required."

Also, Health's internal policies require that OHR strive to process access requests within three business days of receiving the separation forms.

Consequence

Terminated employees who still have access to COV may be able to access other critical programs since it acts as the gateway to all the agency's systems. Untimely removal of WEBVISION access increases the risk that employees could use their inappropriate access to gather sensitive patient information or make unauthorized changes.

Cause

Unit supervisors are not initiating the separation forms in a timely manner resulting in delays in notifying OHR. Currently, when an employee terminates it is the responsibility of the work unit to advise OHR of the departure. Due to the decentralized nature of Health, this does not always happen timely.

Recommendation

Although this issue is a repeat finding, Health has made significant progress and should continue to improve the process surrounding the routing of the separation forms to ensure that system access is removed timely.

Complete System Access Reviews

Severity: Significant Deficiency

Condition

The Division of Disease Prevention (DDP) in the Office of Epidemiology (OEPI) does not periodically review system access to the AIDS Drug Assistance Program (ADAP) database and the e2Virginia system as required by the Security Standard. These systems house demographic and sensitive client information for the HIV Care Formula Grants (Ryan White) federal program.

Criteria

Section 8.1 (AC-2) of the Security Standard details the need for managing information system accounts, stating that organizations must review accounts for compliance with account management requirements at least on an annual basis or more frequently if necessary. Additionally, Health's Security and Confidentiality Policies and Procedures requires that data managers review database account access at least annually and document the findings.

Consequence

The lack of periodic system access reviews increases the risk of unauthorized activity or access to sensitive client information. Health is a decentralized agency and has granted various subrecipients and contractors access to the e2Virginia system as part of their responsibilities under

this program. It is important to perform periodic system access reviews to ensure system access is reasonable and necessary.

Cause

DDP did not follow the Security Standard or Health's Security and Confidentiality Policy relating to access management. While DDP management was aware of the policy, they did not communicate this to the staff performing the work.

Recommendation

DDP should review access to the ADAP database and the e2Virginia systems at least annually and document these reviews accordingly.

Ensure Proper Segregation of Duties Exist with *my*VRS Navigator Access Roles

Severity: Significant Deficiency

Condition

Health has not ensured a proper segregation of duties for employees with *my*VRS Navigator access. The Health employee responsible for generating the monthly Snapshot Confirmation does not have the "Snapshot Processor 2" role within *my*VRS Navigator as recommended. Additionally, a Health employee has both the "Employment Processor" role and "Service Purchase Approver" role, which creates a lack of separation of duties.

Criteria

The Virginia Retirement System (VRS) provides the "Employer Roles and *my*VRS Navigator Security Access" guide which provides descriptions and responsibilities of *my*VRS Navigator access roles. The *my*VRS guide states "the Snapshot Processor 2 generates, views, and confirms the organization's monthly contribution report called a snapshot. It is important that the employee who is the one generating and confirming the monthly snapshot be the employee who holds this role in *my*VRS Navigator." In relation to the Service Purchase Approver role, when an employee holds both the Employment Processor and Service Purchase Approver roles it creates the opportunity for an employee to process fraudulent transactions.

Consequence

The principle of segregation of duties exists as a proper control in order to mitigate risk and ensure employee(s) do not have too much responsibility. When this principal is violated, it creates the opportunity for unauthorized activity.

Cause

Health management does not routinely review *my*VRS Navigator access roles to ensure they are properly assigned among employees and that duties are appropriately segregated.

Recommendation

Health should periodically evaluate *my*VRS Navigator access roles held by its employees to ensure that roles are properly assigned and that segregation of duties between certain roles exist.

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

Health 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 Health, Health 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 Commonwealth's Security Standard. To ensure that Health is properly monitoring third party service providers, we evaluated whether management was properly obtaining, reviewing, and reacting to their service provider audit reports.

Ensure Oversight of Third Party Service Providers

Severity: Significant Deficiency

Condition

Health does not have a consistent process for ensuring third party providers are complying with the Security Standard. The Security Standard considers third-party providers to be organizations that perform outsourced business tasks or functions on behalf of the Commonwealth. As an example, Health relies on a third party vendor for their inventory management, including pricing for year-end inventory. Health has never requested or received a Service Organization Control (SOC) report from the vendor to provide assurance of their processes and internal controls.

In another example, Health implemented a new system, e2Virginia, which stores client eligibility information for the Ryan White program. This system is hosted by a third party vendor and houses sensitive client data. Although the vendor had a SOC report available, Health did not request this report prior to the auditor's request for the report. As a result, Health had no process in place to ensure the third party has adequate internal controls over sensitive client data.

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 Hosted Environment Information Security Standard SEC 525-02, section SA-9-COV-3, states that each agency shall 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. Finally, Topic 10305 of the Commonwealth Accounting Policies and Procedures Manual (CAPP) requires agencies to have adequate interaction with the third party service provider to understand its internal control environment and maintain oversight over the provider to gain assurance over outsourced operations.

Consequence

Health did not maintain sufficient oversight to confirm the provider was complying with the Security Standard requirements. If the controls at these third party providers are not adequate, there is the risk that sensitive information is not properly protected or inventory valuation amounts could be incorrect.

Cause

Health does not have a formal process for identifying third-party service providers and providing appropriate oversight to gain assurance of their third-party providers' environments and internal controls.

Recommendation

Management should develop a process for identifying third party providers and assessing their controls to ensure compliance with state requirements. This process should include the requirement that providers provide documented independent assurances over controls, which could take the form of a SOC report. In addition, a documented review of these assurances should be maintained and provided to all relevant areas of the agency.

Why the APA Audits HIV Care Formula Grants

The HIV Care Formula grant, Part B (Ryan White) program provides approximately $22 million annually to assist the Commonwealth in maintaining a federally authorized AIDS Drug Assistance Program. The program provides insurance, co-pays, and drugs to individuals who cannot afford treatment. We reviewed compliance with time and effort reporting, allowable costs, procurement, reporting and subrecipient monitoring requirements.

Record Accurate Time and Effort Reporting – REPEAT
Severity: Significant Deficiency

Condition

DDP employees did not accurately record their time and effort, which determines the amount of personal service costs that are billed to federal awards for reimbursement. Instead of reporting time and effort based on the actual activity of each employee, DDP employees reported their time each pay period according to an estimate that was determined before the activity was performed.

Criteria

According to the Code of Federal Regulations 45 C.F.R. §75.430 Compensation - Personal Services, costs of compensation are allowable to the extent that they are:

(1) Reasonable for the services rendered and conform to the established written policy of the non-Federal entity consistently applied to both Federal and non-Federal activities.

(2) In compliance with Department of Labor regulations, Fair Labor Standards Act (FLSA) (29 C.F.R. part 516). Records indicating the total number of hours worked each day must support charges for the salaries and wages of nonexempt employees.

Health's internal policy over time and effort also states, "Program directors are responsible for advising staff of the appropriate time and effort codes to be used for their activities. Time shall be reported based on where the effort is applied and not necessarily where the employee is paid."

Consequence

DDP's time and effort documentation does not meet federal requirements or Health's internal policies for supporting charges to the Ryan White grant. This could lead to costs being disallowed by the grantor, leaving the Commonwealth responsible for the costs.

Cause

DDP administrative staff did not properly train program employees on time and effort reporting requirements. Employees improperly reported, and supervisors subsequently approved, time and effort that was not an after the fact distribution of the actual activity of each employee.

Recommendation

This finding was reported in our prior audit report as well as a subsequent review by Health's Internal Audit department. In response to those reviews, DDP has begun implementing corrective action and we recommend they continue with these efforts. Corrective action in progress includes

adopting the time and effort reporting process used by Health's Office of Family Health Services, and improving the supervisory review process for time and effort recorded by employees

Improve Contract Procurement and Management Processes

Severity: Significant Deficiency

Condition

DDP does not comply with procurement policies as set forth in the Agency Procurement and Surplus Property Manual (APSPM). Of 12 contracts tested for proper procurement and management practices, we found:

- Nine of 12 (75 percent) contracts began work prior to signature by an authorized procurement official.
- Contract renewal was not initiated for three of 12 (25 percent) contracts until after the expiration date.
- Five of 12 (42 percent) contracts did not contain timely assignment of a contract administrator.
- Two of 12 (17 percent) contracts contained no documentation of assignment of contract administrator.
- Two of two (100 percent) sole source contracts were not posted in eVA timely.

Criteria

Health is required to comply with the APSPM, which ensures that agencies are in compliance with the Virginia Public Procurement Act. In addition, for information technology purchases Health is required to comply with the Virginia Information Technologies Agency Buy-IT Manual.

Consequence

If contract performance commences prior to signature, there is the risk that performance will include acts outside the scope of the contract. Basic contract law requires offer and acceptance for a contract to be enforceable. If performance begins prior to signature, Health has no authority to require specific performance or to refuse to pay for actions outside the contract scope. In addition, costs incurred for contractors working without proper authorization can be determined to be unallowable. Also, if a contract administrator is not assigned timely, there is the risk that contract performance and billings will be in excess of the contracted amount.

Finally, sole source procurements that are not posted timely are in danger of being protested long after contract commencement. If a protest is upheld, Health could be required to pay protest and re-procurement costs in addition to contract costs.

Cause

DDP procurement personnel are not fully trained on the requirements of the APSPM nor do they rely on the expertise of Health's Office of Procurement and General Services (OPGS) to ensure proper procedures are followed.

Recommendation

DDP needs to improve their contract procurement and management processes, leveraging the experience and expertise of staff in Health's OPGS as needed. Specifically, DDP should develop an internal timeline for each stage of contract processing and follow up with the contractors to ensure that the contracts are executed before the start date of the contract. Staff should consider beginning the contract renewal process at least four to six months in advance of contract expiration to ensure all parties have sufficient time to review and sign renewals and modifications. In addition, DDP staff should communicate with senior management throughout the contract execution process.

Improve Controls over Period of Performance

Severity: Significant Deficiency

Condition

DDP did not maintain adequate, accurate, and consistent documentation to support expenditures by grant period for the Ryan White grant. DDP utilizes a manual process at the end of each grant period to determine which expenses and unliquidated obligations are applicable to a grant period making it difficult to determine not only the proper grant period, but also if federal requirements were met. In addition, DDP did not have adequate support for the grant unliquidated obligations reported on the Federal Financial Report.

Criteria

The Code of Federal Regulations, 2 C.F.R. §200.309 requires that a non-Federal entity may charge to the federal award only allowable costs incurred during the period of performance. The period of performance is defined within the Notice of Award as the grant period.

Consequence

The inability to accurately report obligations and expenditures in the correct period can result in a reduction or loss of funding and questioned costs. In addition, the lack of clear financial information makes it difficult to determine if all grant requirements were met.

Cause

DDP does not use unique project codes for the various grant periods and DDP's manual calculations are not sufficient to determine which expenses are applicable to a grant period. The

practice of maintaining the same project codes between years causes difficulty in determining grant year applicability.

Recommendation

DDP should consider changing project codes to reflect changing grant periods. This is a practice used by other divisions within Health and DDP should adopt this best practice to ensure the financial records provide a clear record of activity by grant period.

Strengthen Subrecipient Monitoring Process

Severity: Significant Deficiency

Condition

DDP did not maintain adequate documentation of subrecipient monitoring reviews. For one subrecipient, corrective action was obtained in March 2016, but was not documented in the subrecipient's review file. Additionally, there was no documentation maintained to support eligibility determinations reviewed as part of the on-site monitoring reviews nor was there evidence of subrecipients conducting required needs assessment.

Criteria

The Code of Federal Regulations, 45 C.F.R. §75.352(d)(2) requires pass through entities (Health) to follow-up and ensure that the subrecipient takes timely and appropriate action on all deficiencies detected through audits and on-site reviews. In addition, the Code of Federal Regulations, 45 C.F.R. §75.352 (d) requires pass-through entities to monitor the activities of the subrecipient to ensure that the subaward is used in compliance with Federal statutes, regulations and terms and conditions of the subaward. Also, 42 U.S. Code §300ff-27(4) requires that a needs assessment is conducted in order to receive grant awards.

Consequence

The inability to monitor subrecipients can result in a reduction or loss of funding and questioned costs. Insufficient monitoring increases the risk of program non-compliance at the subrecipient level. The Commonwealth, through Health, is liable to the federal government for any funds that program subrecipients do not use according to program regulations.

Cause

DDP staff maintain separate procurement, program review and fiscal review files in hardcopy and electronic format for each subrecipient. The ability to ensure accurate and complete information is available for the subrecipient is hampered by not having all information maintained in a single location.

Recommendation

DDP should consider maintaining complete subrecipient files together in a central location. They should also consider establishment of a process to document subrecipient reviews and detailed results of any non-compliance issues. This should be maintained preferably in electronic format so that procurement, program, and fiscal personnel can have central access to determine subrecipient compliance. Finally, DDP should also ensure the required needs assessment is completed by all subrecipients prior to making an award.

Why the APA Audits Hours Worked by Wage Employees

Health employs a significant number of wage employees who are not eligible to participate in the state health insurance plan. Because of the financial penalties associated with violating federal laws pertaining to health insurance coverage, Health management must take necessary precautions to prevent employees from exceeding allowable hours worked thresholds. To determine if the threshold was exceeded, we compared the hours worked by Health wage employees to the hours allowed by the Virginia Acts of Assembly.

Develop and Implement Policy for Monitoring Part-time Hours

Severity: Significant Deficiency

Condition

Health does not adequately monitor wage employee hours to ensure that those employees are limited to 1,500 hours annually. For the monitoring period ended April 30, 2016, there were five part-time employees recording more than 1,500 work hours. Although Health posted various monitoring reporting on the agency's website, there are no policies to ensure that district managers review these reports to make sure their employees do not exceed the 1,500-hour limit. In addition, there were several months where these reports were not generated at all.

Criteria

Chapter 665 § 4-7.01 g. of the 2015 Virginia Acts of Assembly states that "State employees in the legislative, judicial, and executive branches of government, the independent agencies of the Commonwealth, or an agency administering their own health plan, who are not eligible for benefits under the health care plan established and administered by the Department of Human Resource Management ("DHRM") pursuant to Va. Code § 2.2-2818, may not work more than 29 hours per week on average over a twelve month period." DHRM guidance for determining compliance with this requirement defines the Standard Measurement Period as May 1, 2015, through April 30, 2016.

Consequence

Failure to comply with Chapter 665 of the 2015 Virginia Acts of Assembly subjects Health to potential financial penalties for violation of the Federal Affordable Health Care Act by allowing workers to work over the threshold and not receive healthcare benefits.

Cause

It is imperative that district managers maintain an awareness of their wage employees' total hours worked for the year. The lack of a policy requiring that managers review the various monitoring reports resulted in certain wage employees exceeding the 1,500-hour limit.

Recommendation

Health should strengthen their policies and procedures related to the monitoring of wage hours. The policies and procedures should include an alternative method for managers to track their employees' hours in case the monthly and warning reports are unable to generate. Additionally, Health needs to create a process that ensures managers are reviewing the reports that are generated by the Payroll Office

What is a Risk Alert?

During the course of our audit, we encountered an issue that is beyond the corrective action of the Department of Medical Assistance Services' (Medical Assistance Services) management alone and requires the action and cooperation of management and the Commonwealth's Comptroller. The following issue represents such a risk to Medical Assistance Services and the Commonwealth.

Risk Alert – Maintain the Same Payment Transparency that Existed Prior to Cardinal

Medical Assistance Services uses two different systems for processing vendor payments, Oracle and the Medicaid Management Information System (MMIS). Oracle is a typical agency accounting system that interfaces detail payment information to Cardinal, the Commonwealth's Financial Accounting System. MMIS is unique to Medical Assistance Services and it is used to pay Medicaid providers through Medical Assistance Services' fiscal agent. Beginning in fiscal year 2010, management at Medical Assistance Services started processing some of its administrative vendor payments through MMIS; however, the associated detail of these payments were not included in the then accounting system for Virginia, the Commonwealth Accounting and Reporting System (CARS). The following year, 2011, Medical Assistance Services worked with the Department of Accounts (Accounts) to develop a solution to post the details of the MMIS payments to CARS as vendor payments.

As a result of the Commonwealth fully transitioning from CARS to Cardinal in February 2016, we followed up with Medical Assistance Services to determine if the transparency issues from 2010 re-emerged or if management decided to process its administrative contractual expenses directly through Cardinal. Management is continuing to process administrative contractual expenses through MMIS; however, according to management, the resolution agreed upon between Accounts and Medical Assistance Services regarding these administrative payments within CARS is not a feasible solution for Cardinal.

Currently, Medical Assistance Services is reporting the associated detail of these administrative payments within various description fields; therefore, the payments are not directly connected with the associated vendor. Because the payment information cannot be entered as a vendor payment in Cardinal, users of the data outside of Medical Assistance Services management may not be aware that these payments exist. Through public policy decisions, the Commonwealth has decided that its citizens will have access to payment information for administrative contractual expenses through public web sites. The payments in question represent approximately $60 million in administrative contractual expenses annually.

While we recognize that management made these changes to create operational efficiencies, we again encourage Medical Assistance Services to work with the Commonwealth's Comptroller to

examine ways for MMIS payments to be more transparent, user friendly, and available to the citizens of the Commonwealth and oversight agencies.

Why the APA Issued a Comment to Management about CMS-64 Reporting

The CMS-64 report is the one report that Medical Assistance Services must submit to the federal government each quarter that contains the expenditures for which the Commonwealth is entitled to federal reimbursement for the Medicaid Program. In fiscal year 2016, the federal government reimbursed the Commonwealth $4.3 billion. While the federal government extended the reporting deadlines in fiscal year 2016 for CMS-64 reporting, there is no guarantee they will continue to provide extensions in the future. As a result of the importance of CMS-64 reporting and risk that deadlines could be enforced, we have issued this comment to management so that Commonwealth officials are aware of this issue and can take appropriate actions or assume the risk.

Comment to Management – Improve Timeliness of CMS-64 Reporting

Medical Assistance Services is not submitting the Quarterly Statement of Expenditures for the Medical Assistance Program (CMS-64) to the Centers for Medicare and Medicaid Services (CMS) timely. Although management has made improvements in the process of preparing the CMS-64, they requested and were granted extensions by CMS for three quarters during state fiscal year 2016. Of the three quarters, Medical Assistance Services submitted the CMS-64 after the extended deadline in two quarters. The quarterly reports were submitted 36 days after the first quarter ended, 40 days after the second quarter ended, 46 days after the third quarter ended, and 32 days after the fourth quarter ended.

As required by 42 CFR §430.30(c)(1), the CMS-64 report must be prepared quarterly and submitted not later than 30 days after the end of each quarter. However, as stated above, CMS regularly grants extensions to this reporting deadline requirement when requested by Medical Assistance Services.

Historically, CMS has granted reporting extensions for Medical Assistance Services to encourage reporting accuracy that is often diminished by time restrictions. However, CMS could stop granting the extensions at any time and begin implementing various sanctions if reporting deadlines are not met. As stated in 2 CFR Part 200, Subpart D, Section §200.338, if an entity fails to comply with federal statues, regulations, or the terms of the federal award, the federal awarding agency may take one or more of the following actions including, but not limited to:

- Temporarily withholding cash payments pending correction of the deficiency
- Disallowing all or part of the cost of the activity or action not in compliance
- Wholly or partly suspending or terminating the federal award
- Initiating suspension or debarment proceedings
- Withholding further federal awards for the program

Medical Assistance Services' late CMS-64 submissions are caused by several circumstances including external restrictions, timing, complexity, and system changes.

- External Restrictions: When preparing the CMS-64, the Medical Assistance Services' Federal Reporting Unit must gather information from several external sources. Delays often exist when relying on external sources.
- Timing: The general ledger does not close until two weeks into the following quarter. This restriction reduces the amount of time the Federal Reporting Unit has to complete the CMS-64 by two weeks. The information in the general ledger is essential to the accuracy and completeness of the CMS-64.
- Complexity: Because the Commonwealth of Virginia serves its Medicaid enrollees through both the fee-for-service and managed care organization delivery systems, the level of complexity increases to ensure the correct reporting category is used.
- System Changes: During fiscal year 2016, the implementation of the new Cardinal financial system and the loss of a Federal Reporting Analyst contributed to the late submissions.

Although Medical Assistance Services has made improvements in the process of preparing the quarterly CMS-64, management should continue working towards submitting the reports within the 30-day requirement so that potential sanctions imposed by the federal government are not incurred. Additionally, Medical Assistance Services may want to request a more permanent extension to the submission deadline.

Why the APA Audits Access Management for the MMIS

MMIS stores protected health information for nearly one million individuals and it is used to process approximately $8 billion in medical claims annually. While MMIS is operated by a contractor, Medical Assistance Services is the system owner and they are responsible for ensuring that MMIS is managed in accordance with the Commonwealth's Security Standard. To evaluate Medical Assistance Services' management of access for MMIS, we compared internal practices to those required by the Security Standard.

Create Formal Documentation that Facilitates Controlling Privileges in the Medicaid Management Information System – REPEAT

Severity: Significant Deficiency

Condition

Medical Assistance Services has decided to delay implementing the automated process to document MMIS privileges, as defined in its corrective action plan, until 2018. In addition, Medical Assistance Services has not yet completed a conflict matrix documenting the combinations of privileges that create internal control weaknesses in MMIS.

Criteria

The Security Standard, Section 8.1 AC-1, requires agencies to develop, document, disseminate, and review and update annually, formal documented procedures to facilitate the implementation of the access control policy and associated access controls. Additionally, Section 8.1 AC-2(c) and (d) requires that agencies establish conditions for group membership and specify access privileges.

Consequence

Without documenting MMIS conflicting privileges and providing that documentation to the managers reviewing access, management is increasing its risk of granting employees access that violates the concept of separation of duties or the principle of least privileges, which would create internal control weaknesses. In addition, the lack of automated processes to review and document MMIS privileges increases the possibility of omission during user access evaluations. Consequently, the documentation and review of users' assigned privileges continues to be a highly manual process, which increases the risks associated with granting and reviewing users' access. For example, the lack of automated processes to review and document MMIS privileges contributed to Medical Assistance Services' omission of three localities during the annual access review.

Cause

Medical Assistance Services' prior year corrective action plan estimated that the agency would develop an automated process to document MMIS privileges by December 31, 2015. However, following the development of this initial correction plan, the agency instead determined during fiscal year 2015 that the process would not be implemented until 2018, once a new security system was selected for the Medicaid Enterprise System that will replace MMIS. The delay was to avoid using resources on a security system that will be discontinued. Meanwhile, the agency began manually reviewing and updating documented user access privileges, but did not include a conflict matrix to use in evaluating access. The review, which was completed in May 2016, included approximately 3,700 Department of Social Services (Social Services) users, over 800 contractors, and approximately 450 Medical Assistance Services employees.

Recommendation

Medical Assistance Services should continue working towards documenting and evaluating MMIS access. Medical Assistance Services could do this by completing the conflict matrix and incorporating this documentation into the annual access evaluation process to ensure access is properly controlled. Additionally, Medical Assistance Services should apply what it learns in strengthening its management of MMIS access to its replacement, the Medicaid Enterprise System.

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. The Internal Audit Division of Medical Assistance Services contracts these security compliance reviews to outside auditors. We evaluate the results of these audits to ensure issues are addressed and corrective action plans are followed.

Perform Information Technology Review as Required

Severity: Significant Deficiency

Condition

Medical Assistance Services did not obtain the required biennial MMIS security review during fiscal year 2016. The Medicaid program is highly dependent on extensive and complex computer systems that include controls for ensuring the proper payment of Medicaid benefits. These controls reside with the agency as well as with one of Medical Assistance Services' Service Providers (provider).

Criteria

As required by 42 CFR §95.621, Medical Assistance Services must review on a biennial basis its MMIS security program. At a minimum, the review shall include an evaluation of physical and data security operating procedures, and personnel practices.

In addition, 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 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 MMIS, maintained by their provider, are in place and working properly. 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 a provider's environment, which could negatively impact the Commonwealth.

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 assurance that the federal review would satisfy Medical Assistance Services' responsibility. Additionally, according to management, the lack of an information technology auditor has delayed internal audits efforts to ensure the federal and state technology requirements are met.

Recommendation

Medical Assistance Services should ensure that the required biennial review is performed as required. In addition, Medical Assistance Services should use the results of this review to ensure its Provider complies with the requirements in the Security Standard, the Commonwealth Accounting Policies and Procedures Manual (CAPP), the Code of Federal Regulation, and various contracts 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.

Correct Operating Environment and Security Issues Identified by Their Security Compliance Audit – REPEAT

Severity: Significant Deficiency

Condition

Medical Assistance Services Internal Audit Division's review, dated January 31, 2014, found 15 exceptions in which the agency did not comply with the then Commonwealth's Security Standard Security Standard, SEC 501-7.1, and HIPAA Security Rule. According to management's updated correction plan, dated September 30, 2016, the following three exceptions remain and are to be addressed by the following dates:

- Risk Assessment Procedures – December 31, 2016
- Logical Access Controls - December 31, 2016
- Policies and Procedures Reviews - December 31, 2016

Criteria

The prior and current versions of the Security Standard require that all state agencies develop and implement appropriate policies and procedures that meet the minimum standards outlined within it, to include sub-section 6: Risk Management and sub-section 8: Security Control Catalog.

Consequence

As Medical Assistance Services has not yet corrected previously identified weaknesses, the agency continues to maintain an increased risk to its sensitive information systems and data, with regards to confidentiality, integrity, and availability. Critical information systems and data could be

impacted due to the weaknesses identified above, which would hinder Medical Assistance Services' ability to perform its mission-essential functions in support of the Commonwealth.

Cause

As of September 30, 2016, Medical Assistance Services has increased the number of resources necessary to address its information technology security needs and exceptions as reported in the Internal Audit Division's review. However, the magnitude of the changes required and the amount of work necessary have extended the estimated completion date beyond June 30, 2015, as stated in its original corrective action plan. Internal Audit continues to monitor and test implemented corrective actions and management's plans to complete the remaining corrective actions by the end of calendar year 2016.

Recommendation

Medical Assistance Services should continue to follow its updated corrective action plans for the identified weaknesses, which includes developing or acquiring the necessary resources to ensure that appropriate controls are applied over its sensitive information systems and data. In addition, as Medical Assistance Services addresses these weaknesses, the agency should consider the most current Security Standard.

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 Commonwealth's 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

Severity: Significant Deficiency

Condition

Medical Assistance Services does not review 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, in order to ensure the effectiveness of provider controls, Medical Assistance Services' should regularly review Service Organization Control reports and document the results of its reviews.

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 Hosted Environment Information Security Standard SEC 525-02, Section SA-9-COV-3, states that each agency shall 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. Finally, Topic 10305 of the Commonwealth Accounting Policies and Procedures (CAPP) Manual requires agencies to have adequate interaction with the third party service provider to understand its internal control environment and maintain oversight over the provider to gain assurance over outsourced operations.

Consequence

Although Medical Assistance Services maintains a high degree of interactions with its providers, it 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

Medical Assistance Services does not have policies and procedures for reviewing, assessing, and documenting the results of the Service Organization Control reports as a way to evaluate provider 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 to maintain oversight over its providers to confirm they comply with the requirements outlined in their contract, the Security Standards, the CAPP Manual, and industry best practices.

Why the APA Audits Virginia Case Management System (VaCMS) Access

VaCMS is Social Service's new case management system used to control eligibility for approximately one million individuals that receive over eight billion in benefits. During state fiscal year 2016, Social Services delegated control of Medical Assistance Services employee access to Medical Assistance Services' management. Because of the sensitive nature of this data, Medical Assistance Services' management must ensure the integrity and security of the data in the system. To determine if systems access was adequate, we compared Medical Assistance Services' practices to those required by Social Services' and the Commonwealth Information Security Standards.

Review VaCMS Access for Medical Assistance Services Employees

Severity: Significant Deficiency

Condition

Medical Assistance Services Office of Compliance and Security is not reviewing user access to VaCMS. While VaCMS is owned by Social Services, Medical Assistance Services is responsible for assigning and monitoring access for its employees. Specifically, for the seven Medical Assistance Services employees we tested with access to VaCMS:

- Five did not have access consistent with what management approved.
- Five did not have a justification for their access.
- One was approved for a role; however, the access was not granted.
- One had access that was not approved by management.

Criteria

The Security Standard, Section 8.1 AC-2(j), requires an organization to review accounts for compliance with accounts management requirements on an annual basis or more frequently if required to address an environmental change. Additionally, AC-1 Access Control Policy and Procedures requires agencies to develop, disseminate, and review/update annually, formal documented procedures to facilitate the implementation of the access control policy and associated access controls.

Consequence

The lack of VaCMS access reviews significantly increases the risk of unauthorized transactions in VaCMS as well as the risk of granting employees unneeded access; therefore, creating internal control weaknesses.

Cause

Medical Assistance Services did not have the ability to add employees to VaCMS prior to December 2014. Prior to December 2014, Social Services was responsible for granting and monitoring access to VaCMS for Medical Assistance Services' employees. Since this responsibility was transferred to Medical Assistance Services, management has not established formal policies and procedures to operationalize the review of employee access to VaCMS.

Recommendation

Medical Assistance Services should review VaCMS access for its employees. Additionally, management should implement the required VaCMS access policies and procedures to ensure it properly assigns and controls access.

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.

Continue Improving Accounts Receivable Collection Process

Severity: Significant Deficiency

Condition

Medical Assistance Services Fiscal Division is not pursuing collections from providers and recipients timely and in accordance with its policies and procedures. In the cases reviewed from each Program Integrity Unit, Medical Assistance Services' actions have resulted in a delay of possible collections.

Of the 25 Recipient Audit Unit cases reviewed, we found the following:

- Two cases where invoicing letters were not sent timely.
- Six cases where the follow-up collection steps were not completed.
- Two cases that were referred to the Virginia Office of the Attorney General for collection. However, there was no supporting documentation of the referral.
- Two cases where repayment plans were established. However, repayments did not occur, and management did not pursue collection.

Of the five Prior Authorization and Utilization Review (PAUR) mental health provider cases reviewed, we found the following:

- One case where management was not able to provide any documentation to show that collection efforts were made.
- One case where neither a revised payment plan or a negative balance was established.

Of the eight PAUR hospital provider cases reviewed, we found the following:

- One case where invoicing letters were not sent timely.
- Two cases where negative balances were not established timely.

Of the eight Provider Review Unit cases reviewed, we found the following:

- One case where the follow-up collection steps were not completed.

Criteria

Medical Assistance Services' internally established procedures require that it send overpayment notice letters and invoicing letters and collect overpayments from recipients and providers within specified timeframes.

Overpayment notice letters inform recipients to respond within 30 days by writing a check, setting up a repayment plan, or appealing the overpayment notice. The Fiscal Division is to send the recipients' first invoicing letter within five days after notification from the investigation unit. If the recipient does not respond, Medical Assistance Services is to follow up with a series of three additional letters at one day past due, thirty days past due, and sixty days past due.

Overpayment notice letters inform providers to respond within 30 days by writing a check, setting up a repayment plan, or appealing the overpayment notice. If the provider does not respond within 30 days, Medical Assistance Services is to invoice the provider through an invoicing letter. This invoicing letter informs the provider that Medical Assistance Services will collect the overpayment by establishing a negative balance on their account if they do not respond within 30 days.

Consequence

By not following internally established procedures designed to meet 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 on which it is dependent for financial resources.

Cause

Throughout fiscal year 2015, the Accounts Receivable section of the Fiscal Division was understaffed, which resulted in a backlog in the Accounts Receivable area. At the end of fiscal year 2015, Medical Assistance Services contracted with a vendor to provide two accountants to assist with clearing the existing backlog of receivables. As of November 2016, the accountants are still working to clear this backlog. In addition, Medical Assistance Services has currently not completed its implementation of an automated overpayment processing function.

Recommendation

Medical Assistance Services should continue to 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.

Why the APA Audits Information System Security

The Department of Social Services (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 Information Technology (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 Commonwealth's 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

Severity: Significant Deficiency

Condition

Social Services does not consistently apply information security controls across its databases that support sensitive and mission critical Information systems. While Social Services has corrected the control weaknesses identified during the prior year audit in one database, the review of a different database this year also yielded similar control weaknesses. We identified five essential control weaknesses and communicated the details of these weaknesses to management in a separate document marked Freedom of Information Act Exempt (FOIAE) under Section 2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security controls.

Criteria

The Security Standard requires implementing agency specific policies and procedures to establish implementation of consistent controls 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 sensitive Commonwealth data to be compromised by malicious users exploiting those vulnerabilities.

Cause

The lack of appropriate policies and procedures outlining control requirements and the decentralization of systems contributed to the deficiencies identified.

Recommendation

Social Services should dedicate the necessary resources to define and implement the controls discussed in the communication marked FOIAE to meet, at a minimum, the requirements in the Security Standard and industry best practices. Also, Social Services should consider centralizing, to the extent possible, its decentralized information systems to better ensure controls are consistently implemented across all of Social Services' sensitive and mission-critical systems.

Improve Policies, Procedures, and Plans for Backup and Restoration

Severity: Significant Deficiency

Condition

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

Criteria

The Security Standard, Section 8.6 Contingency Planning, requires an agency to conduct backups of information systems in accordance with organization-defined frequency that is consistent with its recovery time and recovery point objectives. The same section of the Security Standard also 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 Business Impact Analysis Requirements, 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

Social Services has not reconciled the Recovery Point Objective (RPO) requirements of the system owners with the services provided by the Partnership. As a result, its policies, as defined by the system owners, do not reflect the current backup and restoration processes performed by the Partnership.

Recommendation

Social Services should align its IT risk management plans (Business Impact Analysis and Risk Management) and IT contingency plans (Continuity of Operations and IT Disaster Recovery Plans) with the current backup and restoration process. While revising the IT risk management and contingency plans, Social Services should complete approved Disaster Recovery Plans that include the requirements to support restoration of systems, data, and applications.

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 Commonwealth's 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.

Improve Oversight of Third Party Service Providers

Severity: Significant Deficiency

Condition

Social Services does not have an established process to maintain oversight over third party IT service 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 Hosted Environment Information Security Standard SEC 525-02, Section SA-9-COV-3, states that each agency shall 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. Finally, Topic 10305 of the Commonwealth Accounting Policies and Procedures (CAPP) Manual requires agencies to have adequate interaction with the third party service provider to understand its internal control environment and maintain oversight over the provider to gain assurance over outsourced operations.

Consequence

Without a documented and established process to gain assurance over third party service providers' internal controls, Social Services cannot consistently validate that those third party service providers have effective security controls to protect its sensitive data. For example, the recent Internal Revenue Service (IRS) review of Social Services' IT environment noted that a Child Support Enforcement vendor did not adequately comply with IRS guidelines for protecting tax information.

Cause

Social Services currently has a process to ensure security requirements are contained within the contracts it has with providers, including the Commonwealth's new Hosted Environment Information Security Standard, SEC 525-02. However, Social Services does not obtain and review independent audit assurance over third party service providers on an ongoing and consistent basis due to a lack of a formal framework.

Recommendation

Social Services should develop and implement a formal framework for gaining appropriate assurance over outsourced operations that impact 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. This process should include the development of formal policies and procedures for obtaining and documenting the evaluation of a reasonable form of assurance to ensure that third party service providers' security controls comply with the requirements described in the Security Standard and documented contract agreement. To maintain consistency and continuity, Social Services should also develop and implement procedures for documenting final decisions and action items that come as a result of the assurance report evaluation process. Finally, Social Services should maintain oversight over this process to confirm compliance with requirements outlined in the Security Standard, CAPP Manual, and industry best practices.

Why the APA Issued a Comment to Management about Records Retention Requirements

Social Services is responsible for the administration of federal and Commonwealth-supported benefit programs, including TANF, SNAP, and Medicaid. Social Services relies on IT systems for proper collection, management, and storing of personal and financial data for use in the operation of these programs. In auditing Social Services' policies governing backup and restoration of IT systems, we found that Social Services has not properly documented and implemented electronic records retention requirements for its sensitive systems. While this matter is not material to the Commonwealth's financial statements or federal programs, we believe it is of sufficient importance to merit management's attention; therefore, we are including it in this report.

Comment to Management - Develop Records Retention Requirements and Processes for Electronic Records

Condition

Social Services does not properly document and implement electronic records retention requirements for its sensitive systems. Specifically, Social Services does not define records retention requirements, nor retain and destroy the records for two sensitive systems. Further, Social Services does not retain and destroy records according to established requirements for a third sensitive system. We communicated the deficiencies to management in a separate document marked FOIAE under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

Criteria

The Virginia Public Records Act requires each agency to be responsible for ensuring that its public records are preserved, maintained, and accessible throughout their lifecycle, including converting and migrating electronic records as often as necessary so that information is not lost due to hardware, software, or media obsolescence or deterioration, section 42.1-91 of the Code of Virginia.

Consequence

Retaining records longer than necessary causes the Commonwealth to spend additional resources to maintain, back-up, and protect the information. Additionally, without documenting and implementing records retention requirements, Social Services is not able to communicate expectations for managing electronic records to its IT department and service providers.

Cause

Although Social Services documents and implements records retention requirements for paper-based information, Social Services has not documented and implemented electronic records retention requirements for its sensitive systems because management would prefer to retain electronic information for as long as possible.

Recommendation

Social Services should identify the retention requirements for the data handled by each sensitive system as discussed in the communication marked FOIAE. Additionally, Social Services should implement a process to ensure consistent compliance with the retention requirements identified for each data set. In developing and implementing records retention requirements for electronic records, Social Services may want to consult with the Library of Virginia.

What is a Risk Alert?

During the course of our audit, we encountered an issue that is beyond the corrective action of agency management alone and requires the action and cooperation of management and the Commonwealth's IT Infrastructure Partnership with Northrup Grumman. The following issue represents such a risk to Health and DBHDS.

Risk Alert – Continue to Upgrade or Decommission End-of-Life Server Operating Systems

The Commonwealth's IT Infrastructure Partnership with Northrop Grumman (Partnership) provides agencies with installation, maintenance, operation, and support of IT infrastructure components, such as server operating systems, routers, firewalls, and virtual private networks. The Partnership is not maintaining some of these devices according to the Security Standard and is exposing the Commonwealth's sensitive data to unnecessary risk.

The Partnership uses end-of-life and unsupported server operating systems in its IT environment to support some of DBHDS and Health's mission critical functions. DBHDS and Health rely on the Partnership to provide current, supported, and updated server operating systems that serve as the foundations for its mission-critical and sensitive systems.

The Security Standard, Section SI-2-COV, prohibits the use of products designated as "end-of-life" by the vendor. A product that has reached its end-of-life no longer receives critical security updates that rectify known vulnerabilities that can be exploited by malicious parties.

The Partnership maintains and administers 56 server operating systems for DBHDS and two server operating systems for Health that are officially designated as end-of-life per the vendor. The Partnership's use of unsupported server operating systems increases the risk that existing vulnerabilities will persist in the server operating systems without the potential for patching or adequate mitigation. These unpatched vulnerabilities increase the risk of cyberattack, exploit, and data breach by malicious parties. Additionally, vendors do not offer operational and technical support for server operating systems designated as end-of-life, which increases the difficulty of restoring system functionality if a technical failure occurs.

DBHDS and Health are aware of this issue and are working with the Partnership to develop remediation plans to upgrade or decommission the end-of-life server operating systems. Until then, the agencies and the Partnership have installed additional security controls to attempt to reduce some of the risk that the end-of-life server operating systems introduce into the IT Environment.

DBHDS and Health should continue working with the Partnership to upgrade or decommission all of the end-of life server operating systems as soon as possible. Doing this will further reduce the risk to the confidentiality, integrity, and availability of sensitive Commonwealth data and achieve compliance with the Security Standard.

Commonwealth of Virginia

Auditor of Public Accounts

Martha S. Mavredes, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 15, 2016

The Honorable Terence R. McAuliffe
Governor of Virginia

The Honorable Robert D. Orrock, Sr.
Vice-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 section below, for the year ended June 30, 2016. 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, 2016, and test compliance for the Statewide Single Audit. In support of this objective, we evaluated the accuracy of recorded financial transactions in the Commonwealth Accounting and Reporting System, Cardinal, each agency's accounting system, and other financial information they reported to the Department of Accounts; reviewed the adequacy of each agency's 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
- Federal revenues, expenses, and compliance for:
  - Block Grants for Prevention and Treatment of Substance Abuse
- Operational expenses
- Payroll expenses
- Institutional revenues
- Community Service Board contracts
- Information system security
- Systems access controls
- *my*VRS Navigator

Department of Health

- Accounts receivable
- Inventory
- Federal revenues, expenses, and compliance for:
  - HIV Care Formula Grants
  - Immunization Cooperative Agreements
- 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
- *my*VRS Navigator

Department of Medical Assistance Services

Federal revenues, expenses, and compliance for the Medicaid program
Accounts receivable
Accounts payable
Contract management
System access controls
Utilization units
*my*VRS Navigator

Department of Social Services

Federal revenues, expenses, and compliance for:
- Foster Care
- Adoption Assistance
- Social Services Block Grant

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
*my*VRS Navigator

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 covered by this report:

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 of the Secretary of Health and Human Resources' 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, contracts, reconciliations, and board minutes; and observation of each agency's operations. We tested transactions and system access and 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 of transactions 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 Accounting and Reporting System, Cardinal, each agency's accounting system, and other financial information they reported to the Department of Accounts for inclusion in the Comprehensive Annual Financial Report for the Commonwealth of Virginia. These agencies record their financial transactions on the cash basis of accounting, which is a comprehensive basis of accounting other than accounting principles generally accepted in the United States of America. The financial information presented in this report came directly from the Commonwealth Accounting and Reporting System.

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 sections for each agency, we identified certain deficiencies in internal control that we consider to be material weaknesses in internal control 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 consider the following deficiencies in internal controls over financial reporting in the sections for each agency to be **material weaknesses**:

Department of Behavioral Health and Developmental Services

- Improve Controls over Financial Reporting

Department of Health

- Improve Inventory Valuation Procedures

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 consider the deficiencies, other than those mentioned above, and classified with a severity of "Significant Deficiency" in the sections for each agency, to be significant deficiencies.

All findings in the sections for each agency, which are classified as a material weakness or significant deficiency, contain the results of our tests that disclosed instances of noncompliance or other matters that are required to be reported under Government Auditing Standards.

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 Statewide Single Audit, but are of sufficient importance to warrant the attention of those charged with governance. These deficiencies are in the sections for each of the applicable agencies and have a severity classification of "Deficiency."

The material weakness or significant deficiency findings for the Agencies of the Secretary of Health and Human Resources will have the same classification for the Commonwealth. As a result, 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 Commonwealth of Virginia Single Audit Report for the year ended June 30, 2016.

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 in this report as "REPEAT."

Exit Conference and Report Distribution

We discussed this report with management at the Agencies of the Secretary of Health and Human Resources 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

GDS/clj

COMMONWEALTH of VIRGINIA

JACK BARBER, M.D.
INTERIM COMMISSIONER

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.

SUBJECT: *Responses to FY 2016 HHR Report*

DATE: January 15, 2017

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

Risk Alert - Properly Plan for CIPPS Replacement

On January 19, 2017, the Department received VITA's Procurement Governance Request (PGR) Approval to enter into a sole source agreement with Kronos. Our Procurement office estimates four weeks to complete the sole source contract. The vendor's draft Statement of Work for the upgrade is 16 weeks. Based on this information, the Department is targeting mid June 2017 to complete the upgrade.

It should be noted that the Department does not currently have a Business Analyst assigned to the Cardinal Payroll project. This position is necessary to review the different versions of KRONOS to assess the requirements needed for the new version. This position is not funded and the Department is looking for resources to allow for recruitment.

The Department is currently receiving systems support over KRONOS which will expire on June 30, 2017, even though there is not a current agreement with the vendor. The PGR Approval will delegate authority to extend the support to January 31, 2019, beyond the end date of the Cardinal Payroll Project.

The Department acknowledges that difficulties exist at our Central Office around the areas of reconciliations and the processing of federal transactions. The Department did not experience these issues at any of our facilities, and we believe that the difficulties are not related to the Cardinal Financials interfaces that the facilities and central office share.

While reviewing completed projects will usually provide for areas of improvement regarding project management, the Department feels that despite previous difficulties, that it will effectively execute the KRONOS upgrade and interface work related to the Cardinal Payroll project.

Improve Controls over Financial Reporting

DBHDS concurs with the comment. DBHDS will ensure that the Offices of Administrative Services, Architecture and Engineering, Budget and Financial Reporting and Fiscal Services collaborate on the calculation of contractual commitments at fiscal year end. In addition, the attachment that shows the amount of contractual commitments that DBHDS has at year-end will be submitted to the Office of Internal Audit for review.

Continue to Improve IT Governance – REPEAT, Continue to Upgrade Unsupported Technology – REPEAT, Develop Baseline Configurations for Information Systems – REPEAT

DBHDS concurs with the comment. The funding request to remediate the audit finding (Audit Remediation Decision Package) was rejected and final corrective action plans are dependent on funding. DBHDS will review options available when the final budget is approved. Previously the Department instituted the FAIR Project with a strategy to engage an executive-level decision team. The decision team would provide guidance in selecting a core suite of common applications that will be supported by the Central Office, then migrate all facility users to that suite. The remaining facility-specific applications will be modernized and migrated to the agency-wide infrastructure environment at VITA, then all agency applications will be transitioned to a cloud hosting provider using the VITA server hosting multi-supplier model. 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. It is expected that the reduction in DBHDS sensitive IT systems will continue.

Improve SQL Database Security – REPEAT

DBHDS concurs with the comment. The funding request to remediate the audit finding (Audit Remediation Decision Package) was rejected and final corrective action plans are dependent on funding. DBHDS will review options available when the final budget is approved.

Improve Access Controls over Financial Management System – REPEAT

The Department concurs with the audit comment. DBHDS will enhance and establish where needed; policies, procedures, and controls over system access to FMS including the documenting of critical ledgers and roles in the newest FMS version to ensure proper separation of duties. In

addition, DBHDS will address controls related to times when it is necessary to assign conflicting roles to an individual to also ensure proper separation of duties. DBHDS will update the form used to request, change, and delete access to FMS so that it agrees with the design of the upgraded system. DBHDS will also develop a process to monitor access to the new FMS version, annually for all regions and facilities. Finally DBHDS will continue with efforts to ensure access forms are completed properly, access granted is reasonable and access for terminated employees is removed timely.

Improve Internal Controls Surrounding Sensitive Documents

The Department concurs with the audit comment. DBHDS will ensure that The Commonwealth's Information Security Standard, SEC501-09, Section SC-8-COV is adhered to when sensitive data is transmitted to any external agency or entity. To complete this, DBHDS Information Security Office will be leading two initiatives to mitigate this risk. To assure information sent via email is encrypted (internally and externally), we are reviewing options that would push out Microsoft Outlook settings to all users assuring all emails are digitally signed and all content and attachments are encrypted for outgoing messages. To follow a layered defense approach, we are currently in the process of creating a group policy and security group to provide users that regularly send sensitive data, a file compression application that will give them the ability to encrypt all attachments. In addition, upon receiving the information from the APA reviewer, a ticket was opened with VITA on September 30, 2016. Following the subsequent confirmation received from VITA, encryption tools were installed on the devices used by staff who routinely process sensitive information.

Improve Controls over *myVRS* Navigator – REPEAT

The Department concurs with the audit comment and will ensure that VNAV snapshot reconciliations are completed timely and include all aspects of a reconciliation between CIPPS, PMIS and VNAV. DBHDS will also ensure that policies and procedures adequately describe how the reconciliations of CIPPS and PMIS to VNAV are to be completed.

Regarding the issue of improper access to VNAV. DBHDS will continue to ensure that proper segregation of duties is in place related to access to VNAV. The agency feels that controls are in place as there was only one employee, out of 18 tested, that was found to have improper access to VNAV.

Enhancements to policies and procedures and a review of access to VNAV at DBHDS Central Office and all facilities will be completed in FY 2017. DBHDS Central Office and Facilities will continue to work on the monthly reconciliations between CIPPS, PMIS and VNAV to ensure they are properly completed and include all required documentation.

Improve Controls Over Payroll – REPEAT

Department concurs with the audit comment. The DBHDS Office of Internal Audit conducted this testwork and has reviewed the responses given by the facilities and Central Office to the findings

noted. The Department has agreed with the responses to the findings and will be completing follow-up reviews to ensure compliance.

Improve Internal Controls Surrounding At-Will Employees

The Department concurs with the audit comment. A process will be put in place to track leave balance certifications from At-Will employees and DBHDS HR will ensure that DBHDS At-Will employees certifiy their leave balances after January 12th of each year for the previous year. In the event of an DBHDS AT-Will employee transferring to another state agency, DBHDS will ensure that a certification of leave balances will be provided to that agency by DBHDS HR.

Comply with the *Code of Virginia* Economic Interest Requirements – REPEAT

The Department concurs with the audit comment. The Department will continue to work toward ensuring all employees required to submit the Statement of Economic Interest form do so timely and also that they complete the required Conflict of Interest Training. DBHDS has developed a process where the individuals required to file the Statement of Economic Interest form will be tracked along with their timely completion of the Conflict of Interest Training. DBHDS will require employees to take the Conflict of Interest Training that is offered and accounted for through the DBHDS Knowledge Center.

Improve Controls over Intangible Assets – REPEAT

DBHDS concurs with the comment. Policies for Intangible Asset Accounting and Reporting were developed during FY 2016. The policy identifies what constitutes an intangible asset, how they will be identified and the responsible parties. DBHDS concurs that the method to track intangible assets and the timing are not specified in the policies. The entire policy is currently being reviewed and revised.

Since the end of September 2016, responsibility of tracking and reporting intangible assets has shifted. The policies have been reviewed and are in the process of being revised. A monthly meeting involving IS&T and Fiscal has been established to discuss new, ongoing and future projects and software purchases. We believe these changes will address the APAs concerns and resolve this issue.

Improve Policies and Procedures over Fixed Assets – REPEAT

DBHDS concurs with the comment. Policies and procedures related to all aspects of Fixed Assets (Departmental Instruction 840) have been under development since May 2015, and are still being refined in FY 2017. DBHDS is committed to providing clear, concise intructions as they relate to the appropriate management of state property.

Improve Controls over Sale of Land – REPEAT

DBHDS concurs with the comment. DBHDS will ensure that there are adequate policies and procedures that cover all aspects related to the sale of land. It must be noted that the sale of land belonging to the Commonwealth is the responsibility of the Department of General Services (DGS). DBHDS will continue to work with DGS, the Office of the Attorney General, the

Department of Treasury and the facilities with FAACS responsibility to ensure that land sales are recorded according to the Department of Accounts (DOA) regulations.

Improve Internal Controls over Fixed Asset Additions – REPEAT

DBHDS concurs with the comment. DBHDS has made progress in recording assets timely and accurately as shown by the large decrease in the error rate found during the audit. DBHDS will continue to work toward compliance regarding the accuracy and timeliness of the recording of fixed assets. DBHDS will also ensure that communication is enhanced regarding assets being moved from CIP to the proper depreciable capital asset category.

cc: Jack Barber, M.D., DBHDS Interim Commissioner
Kathy Drumwright, DBHDS Interim Chief Deputy Commissioner
Connie Cochran, DBHDS Assistant Commissioner for Developmental Services
Don Darr, DBHDS Assistant Commissioner for Finance and Administration
Daniel Herr, DBHDS Assistant 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
Ken Gunn, DBHDS Director of Budget and Financial Reporting
Dan Hinderliter, DBHDS Director of the Office of Administrative Services
Phil Peter, DBHDS Director of Fiscal and Grants Management
Stacy Pendleton, DBHDS Assistant HR Director
Chris Sarandos, DBHDS Chief Information Officer
Randy Sherrod, DBHDS Internal Audit Director

COMMONWEALTH of VIRGINIA

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

Department of Health
P O BOX 2448
RICHMOND, VA 23218

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

January 4, 2017

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, 2016. 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 SOCIAL SERVICES

Office of the Commissioner

Margaret Ross Schultze
COMMISSIONER

January 11, 2017

Ms. 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 2016 review by the Auditor of Public Accounts.

Should you require additional information, please do not hesitate to contact Jack B. Frazier, Deputy Commissioner, Operations, by e-mail at jack.b.frazier@dss.virginia.gov or by telephone at (804) 726-7384.

Sincerely,

Margaret Ross Schultze

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

COMMONWEALTH of VIRGINIA

Department of Medical Assistance Services

CYNTHIA B. JONES
DIRECTOR

SUITE 1300
600 EAST BROAD STREET
RICHMOND, VA 23219
804/786-7933
800/343-0634 (TDD)
www.dmas.virginia.gov

January 19, 2017

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, 2016. We concur with the audit findings assigned to DMAS. Attached please find the Department's Corrective Action Plan for the DMAS FY 2016 audit findings.

We appreciate the collaborative effort and the constructive feedback from your audit team during this year's audit. If you have any questions, please do not hesitate to contact our Director of Internal Audit, Paul Kirtz.

Sincerely,

Cynthia B. Jones

Risk Alert - Maintain the Same Payment Transparency that Existed Prior to Cardinal (issued as MP #2)

Medical Assistance Services uses two different systems for processing vendor payments, Oracle and the Medicaid Management Information System (MMIS). Oracle is a typical agency accounting system that interfaces detail payment information to Cardinal, the Commonwealth's Financial Accounting System. MMIS is unique to Medical Assistance Services and it is used to pay Medicaid providers through Medical Assistance Services' fiscal agent. Beginning in fiscal 2010, management at Medical Assistance Services started processing some of its administrative vendor payments through MMIS, however the associated detail of these payments were not included in the then accounting system for Virginia, the Commonwealth Accounting and Reporting System (CARS). The following year, 2011, Medical Assistance Services worked with the Department of Accounts (Accounts) to develop a solution to post the details of the MMIS payments to CARS as vendor payments.

As a result of the Commonwealth fully transitioning from CARS to Cardinal in February 2016, we followed up with Medical Assistance Services to determine if the transparency issues from 2010 reemerged or if management decided to process its administrative contractual expenses directly through Cardinal. Management is continuing to process administrative contractual expenses through MMIS, however according to management, the resolution agreed upon between the Accounts and Medical Assistance Services regarding these administrative payments within CARS is not a feasible solution for Cardinal.

Currently, Medical Assistance Services is reporting the associated detail of these administrative payments within various description fields, therefore the payments are not directly connected with the associated vendor. Because the payment information cannot be entered as a vendor payment in Cardinal, users of the data outside of Medical Assistance Services management may not be aware that these payments exist. Through public policy decisions, the Commonwealth has decided that its citizens will have access to payment information for administrative contractual expenses through public web sites. The payments in question represent approximately $60 million in administrative contractual expenses annually.

Recommendation

While we recognize that management made these changes to create operational efficiencies; we again encourage Medical Assistance Services to work with the Commonwealth's Comptroller to examine ways for MMIS payments to be more transparent, user friendly, and available to the citizens of the Commonwealth and oversight agencies.

Corrective Action Plan:

To ensure transparency, the Department will publish administrative vendor payments processed in the MMIS system on the agency website. Published information will include the vendor name, payment amount, payment date, program, and expenditure object code. The Department will include this information for payments dating back to February 1, 2016 when the Cardinal system went live. The website will be updated at the beginning of each month to include the most current payments through the preceding month. The source of information will be the Apex database of MMIS payments.

Responsible Persons:

- Karen Stephenson, Controller, DMAS Fiscal and Purchases Division
- Keith Collins, General Ledger Manager, DMAS Fiscal and Purchases Division

Estimated Implementation Date: March 31, 2017

Comment to Management - Improve Timeliness of CMS-64 Reporting (issued as MP #7)

The Department of Medical Assistance Services (Medical Assistance Services) is not submitting the Quarterly Statement of Expenditures for the Medical Assistance Program (CMS-64) to the Centers for Medicare and Medicaid Services (CMS) timely. Although management has made improvements in the process of preparing the CMS-64, they requested and were granted extensions by CMS for three quarters during fiscal year 2016. Of these three quarters, Medical Assistance Services submitted the CMS-64 after the extended deadline in two quarters. The quarterly reports were submitted 36 days after the first quarter ended, 40 days after the second quarter ended, 46 days after the third quarter ended, and 32 days after the fourth quarter ended.

As required by 42 CFR §430.30(c)(1), the CMS-64 report must be prepared quarterly and submitted not later than 30 days after the end of each quarter. However, as stated above, CMS regularly grants extensions to this reporting deadline requirement when requested by Medical Assistance Services.

Historically, CMS has granted reporting extensions for Medical Assistance Services to encourage reporting accuracy that is often diminished by time restrictions. However, CMS could stop granting the extensions at any time and begin implementing various sanctions if reporting deadlines are not met. As stated in 2 CFR Part 200, Subpart D, Section §200.338, if an entity fails to comply with federal statues, regulations, or the terms of the federal award, the federal awarding agency may take one or more of the following actions including, but not limited to:

- Temporarily withholding cash payments pending correction of the deficiency

- Disallowing all or part of the cost of the activity or action not in compliance
- Wholly or partly suspending or terminating the federal award
- Initiating suspension or debarment proceedings
- Withholding further federal awards for the program

Medical Assistance Services' late CMS-64 submissions are caused by several circumstances including external restrictions, timing, complexity, and system changes.

- External Restrictions: When preparing the CMS-64, the Medical Assistance Services' Federal Reporting Unit must gather information from several external sources. Delays often exist when relying on external sources.

- Timing: The general ledger does not close until two weeks into the following quarter. This restriction reduces the amount of time the Federal Reporting Unit has to complete the CMS-64 by two weeks. The information in the general ledger is essential to the accuracy and completeness of the CMS-64.

- Complexity: Because the Commonwealth of Virginia serves its Medicaid enrollees through both the fee-for-service and managed care organization delivery systems, the level of complexity increases to ensure the correct reporting category is used.

- System Changes: During fiscal year 2016, the implementation of the new Cardinal financial system and the loss of a Federal Reporting Analyst contributed to the late submissions.

Recommendation

Although Medical Assistance Services has made improvements in the process of preparing the quarterly CMS-64, management should continue working towards submitting the reports within the 30-day requirement so that potential sanctions imposed by the Federal government are not incurred. Additionally, Medical Assistance Services may want to request a more permanent extension to the submission deadline

Corrective Action Plan:

Corrective action is complete. DMAS will continue to request an extension in advance if needed. If CMS denies the request, we will submit the report on time and explain that any corrections will be completed on the next submission. CMS has emphasized on several occasions that accuracy is more important than timeliness when it comes to the CMS certification. To date CMS has always granted DMAS an extension. If CMS was to deny this request, DMAS would adhere to the 30 day reporting deadline. As a result, federal funds would never be endangered.

We discussed the possibility of a more permanent extension to the submission deadline with the CMS Report Analyst. The response was that it is not possible and an extension is granted on a case by case basis.

Responsible Persons:

- Karen Stephenson, Controller, DMAS Fiscal and Purchases Division
- Shionda Scott, Federal Reporting Manager, DMAS Fiscal and Purchases Division

Implementation Date: December 31, 2016

Create Formal Documentation that Facilitates Controlling Privileges in the Medicaid Management Information System – Repeat (issued as MP #1)

Condition

Medical Assistance Services has decided to delay implementing the automated process to document MMIS privileges, as defined in its corrective action plan, until 2018. In addition, Medical Assistance Services has not yet completed a conflict matrix documenting the combinations of privileges that create internal control weaknesses in MMIS.

Recommendation

Medical Assistance Services should continue working towards documenting and evaluating MMIS access. Medical Assistance Services could do this by completing the conflict matrix and incorporating this documentation into the annual access evaluation process to ensure access is properly controlled. Additionally, Medical Assistance Services should apply what it learns in strengthening its management of MMIS access to its replacement, the Medicaid Enterprise System.

Corrective Action Plan:

DMAS' Office of Compliance and Security (OCS) has developed a manual process used in 2016, to review MMIS (also known as VAMMIS) privileges with all groups. This manual process has been used to make sure the documentation includes all steps, and works as intended. For example, the intent is to make sure, the process is well-documented, and can be used by anyone within OCS.

Improvement Phases:

Phase I: DMAS reviewed all user access with DMAS Managers, Supervisors and Division Directors, explaining and provided on the spot training to ensure those reviewers, understood what was asked for during the review (Completed June 14, 2016).

The following actions were completed:

1. All MMIS user requests are documented.
2. Annual reviews are conducted, with detail reports, identifying what is in the cluster and describes what the user has access to.
3. OCS met with supervisors, managers, Division Directors as well as an IM Systems Analyst who understands the MMIS transactions, were conducted to discuss current access and modifications needed. Based on the meetings, OCS will develop the conflict matrix (see Phase II).

Phase II: The OCS ISO is reviewing current access from assigned clusters, to design Roles from those clusters. In parallel, a Conflict Matrix is also being created (Estimated completion is March 31, 2017).

Responsible Persons:

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

Estimated Implementation Date: March 31, 2017

Perform Information Technology Review as Required (issued as MP #8)

Condition

Medical Assistance Services did not obtain the required biennial MMIS security review during fiscal year 2016. The Medicaid program is highly dependent on extensive and complex computer systems that include controls for ensuring the proper payment of Medicaid benefits. These controls reside with the agency as well as with one of Medical Assistance Services' Service Providers (Provider).

Recommendation

Medical Assistance Services should ensure that the required biennial review is performed as required. In addition, Medical Assistance Services should use the results of this review to ensure its Provider complies with the requirements in the Security Standard, the

Commonwealth Accounting Policies and Procedures Manual (CAPP), the Code of Federal Regulation, and various contracts 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 is in the process of procuring a security audit of the MMIS. 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 MMIS that started in September 2015. The 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 on April 28, 2016, the auditors reported they had assessed the following items:

- The Commonwealth's policies and procedures
- The Contractor's policies and procedures
- Network system security
- Information systems virus protection capabilities
- Information systems security patch management
- Logical access controls
- Network device controls (firewalls, routers, and switches)
- Web application and website security
- Database controls
- Remote access controls

While DMAS still has not received the draft audit report from the OIG, the DMAS Information Management Division and the Service Provider have been working diligently to address the audit issues and system vulnerabilities that were presented in field work exit conference.

Due to strained resources for both the Service Provider and DMAS in responding to the audit requests and resolving the audit issues, DMAS choose not to begin another similar security audit while the Federal security audit was still in process. 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 MMIS.

DMAS is working 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 provided the Statement of Requirements (SOR) to CAI on September 15, 2016. CAI received a Statement of Work (SOW) response from one

vendor on October 17, 2016. No other vendors submitted a SOW. After reviewing the SOW submitted by the vendor, DMAS selected the vendor and began negotiations with the vendor. Modifications are being made to the SOW and the negotiations should be completed by January 31, 2017.

The security audit as described in the SOR will ensure that the DMAS is in compliance with the following audit requirements for MMIS:

- 45 CFR §95.621 (f) (3) – *ADP System Security Reviews*
- 45 CFR §164.308 (a) (8) – *Standard Evaluation*
- Code of Virginia §2.2 – 2009.A 1 – Address the scope and frequency of security audits

The results of the OIG Audit and the security audit will help 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.

Responsible Persons:

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

Estimated Implementation Date: September 1, 2017

Correct Operating Environment and Security Issues Identified by their Security Compliance Audit – Repeat (issued as MP #3)

Condition

Medical Assistance Services Internal Audit Division's review, dated January 31, 2014, found 15 exceptions in which the agency did not comply with the Security Standard, SEC 501-7.1, and HIPAA Security Rule. According to management's updated correction plan, dated September 30, 2016, the following 3 exceptions remain and are to be addressed by the following dates:

- Risk Assessment Procedures – December 31, 2016
- Logical Access Controls - December 31, 2016

- Policies and Procedures Reviews - December 31, 2016

Recommendation

Medical Assistance Services should continue to follow its updated corrective action plans for the identified weaknesses, which includes developing or acquiring the necessary resources to ensure that appropriate controls are applied over its sensitive information systems and data. In addition, as Medical Assistance Services addresses these weaknesses, the agency should consider the most current Security Standard, SEC 501-09.

Corrective Action Plan:

The original DMAS security compliance audit referenced in the APA report contained 15 findings, 12 findings have been resolves and DMAS is in process of completing corrective action for the three remaining findings that have not yet been fully addressed:

Risk Assessment Procedures – extended due date: December 31, 2017

During FY 2016, DMAS tested its risk assessment process for seven (7) internal application reviews. Risk Management Treatment Plans have also been identified, documented, and discussed with the Contract Monitors. The Office of Compliance and Security (OCS) has followed up in December 2016, reminding the Contract Monitors that their Treatment Plans are expected to be taken to resolution.

OCS will conduct internal Risk Assessments on the remaining applications listed on the DMAS IT Security Audit Plan dated 7/8/16 (updated annually), and listed as required in VITA CSRM (Commonwealth Enterprise Technology Repository (CETR)/Archer.

OCS is reviewing and developing an internal documented procedure to complete these internal application Risk Assessments as well as have any Risk Management Treatment Plans resolved, by end of calendar year, December 31, 2017.

Logical Access Controls - extended to February 28, 2017

The Internal Audit Security Compliance audit report recommended the following five actions to be taken:

1. Review the user accounts identified for the TPLRS, HCOSTS, FAIR and CAS-E applications that did not have access request and authorizations forms to ensure access is appropriate for these users. Subsequently, these users' access should be documented on the required access request forms or be removed, if access is no longer needed.

OCS Response: These four internal Oracle applications, TPLRS, HCOSTS, FAIR and CAS-E, account access reviews including documentation, will be completed by January 31, 2017.

2. Implement procedures to document access requests and authorizations for the CAS-E application.

   OCS Response: To be completed by January 31, 2017 for this internal application, including documentation. Documentation to be updated as required. Procedures to be developed for quarterly/annual reviews, as required by policy.

3. Implement procedures for ensuring the necessary access agreements are obtained, recorded and retained prior to access being granted to DMAS information systems.

   OCS Response: Documentation and procedures are being updated as required by policy as part of DMAS COV annual review (described below; to be completed by January 31, 2017).

4. Ensure the active DMAS network (Active Directory) and FAIR application user accounts are disabled or removed that belong to the terminated employee identified.

   OCS Response: COV annual reviews were sent to Division Directors on December 2, 2016, with requested responses due 12/16/16, 12/19/16, and extended due date through 1/6/17 due to Holidays.

   OCS will consolidate responses and take action to update user access as defined by DMAS Division Directors, and, develop policy and procedures to continue annual reviews as required. Completion expected by January 31, 2017.

5. Identify the appropriate IM or business owners responsible for performing user access reviews, and coordinate with the responsible owners to develop and implement procedures requiring application or system owners to perform user access reviews on a periodic basis to identify user accounts that are not appropriate, including: inappropriate user access rights, roles and privileges assigned to accounts; unnecessary accounts that are no longer needed or used; and inactive or terminated accounts. These procedures should provide specific guidelines for conducting user access reviews, such as: reviewing all user accounts and the corresponding access rights on a specified, periodic – at least annual - basis, especially accounts that have privileged roles; following-up on any discrepancies or issues found, signing off on the review confirming that access is appropriate, and retaining documentation of these reviews.

OCS Response: Similar to Item #5 above. Procedures are being developed for COV and applications, annual reviews required by policy, to be completed by February 28, 2017.

Policies and Procedures Reviews ---extended to January 31, 2017

DMAS continues to review and finalize the required policies by SEC501-09. Documents below are numbered for convenience only. Document numbers 1-18 match SEC501 "Families of Controls".

1. 1-7 have been finalized, signed by Agency Head and posted to MOAT.

    1. DMAS Access Control
    2. DMAS Security Awareness and Training
    3. DMAS Audit and Accountability
    4. DMAS Security Assessment and Authorization
    5. DMAS Configuration Management
    6. DMAS IT Contingency Planning
    7. DMAS Identification and Authentication

2. 9-13 have been approved by DMAS Security Advisory Committee (SAC) but pending Agency Head signature.

    9. System Maintenance
    10. Media Protection
    11. Physical and Environmental Protection Policy
    12. Security Planning
    13. Personnel Security

3. 14-16 have been sent to the SAC for a vote via email (i.e., e-vote) by 1/17/17.

    14. Risk Assessment
    15. System and Services Acquisition
    16. System and Communications Protection
    17. IT System and Information Integrity
    18. Security Program Management

4. Policy 8 (for Incident Response) is still being finalized.

Additional Supplemental policies are being drafted, reviewed by the Policy Owner, and then sent to the DMAS SAC for a review and an e-vote. Documents are numbered below for ease of reference only. They include (but are not listed in any particular order):

S1.DMAS COV-owned and Non-COV-Owned Mobile Device Security and Use Policy, dated 10/15/14, to be reviewed every 3 years.
S2.DMAS Information Resource Acceptable Use Policy (with use acknowledgement agreement)
S3.Social-Media Policy
S4.Security Incident Response Policy and Procedure
S5.DMAS Enterprise Security Policy, Standards and Procedures
S6.DMAS HIPAA Security Policy, dated 06/05/13, pending review and revision
S7.DMAS SSP, Medicaid Enterprise System (MES) Master Security Plan (MSP) (as required by CMS)
S8.DMAS Privacy Impact Analysis (PIA) (including template privacy impact for social media)
S9.DMAS Business Impact Analysis (BIA)
S10.DMAS Risk Assessment (RA) Policy and Procedure and Template
S11.DMAS Guest WiFi Acceptable Use Policy
S12.Annual COOP required by 4/1/17
S13.Annual Disaster and HIPAA Contingency Plan review and update.

Once approved and signed, these documents will be posted for staff via MOAT. These policies have been marked for annual review where required, to address "review" delays in the past.

Responsible Persons:

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

Estimated Implementation Dates:

Risk Assessment Procedures – December 31, 2017
Logical Access Controls – February 28, 2017
Policies and Procedures Reviews – January 31, 2017.

Review and Document Service Organization Control Reports of Third-Party Service Providers (issued as MP #5)

Condition

Medical Assistance Services does not review 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, in order to ensure the effectiveness of Provider controls, Medical Assistance Services' should regularly review Service Organization Control reports and document the results of its reviews.

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 to maintain oversight over its Providers to confirm they comply with the requirements outlined in their contract, the Security Standards, the CAPP, and industry best practices.

Corrective Action Plan:

To ensure proper oversight of Service Providers who provide significant fiscal processes, DMAS will take the following steps:

1. DMAS will develop policy and procedures to ensure that the Service Organization Control (SOC) reports received for service providers who provide significant fiscal processes for the agency are reviewed, assessed and documented. (to be completed by December 31, 2017)

2. Procurement will define procedures to perform periodic follow-up reviews of SOC Report issues/findings until they are remediated. (to be completed by December 31, 2017)

3. Procurement will coordinate training for the Contractor Administrators and develop guidelines and worksheets for Administrators to use to document reviews of the SOC Reports. (to be completed by March 31, 2018)

Responsible Persons:

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

Estimated Implementation Date: March 31, 2018

Review VaCMS Access for Medical Assistance Services Employees (issued as MP #6)

Condition

Medical Assistance Services Office of Compliance and Security is not reviewing user access to VaCMS. While VaCMS is owned by Social Services, Medical Assistance Services is responsible for assigning and monitoring access for its employees. Specifically, for the seven Medical Assistance Services employees we tested with access to VaCMS:

- Five did not have access consistent with what management approved.
- Five did not have a justification for their access.
- One was approved for a role; however, the access was not granted.
- One had access that was not approved by management.

Recommendation

Medical Assistance Services should review VaCMS access for its employees. Additionally, management should implement the required VaCMS access policies and procedures to ensure it properly assigns and controls access.

Corrective Action Plan:

DMAS will perform a review of DMAS employees' VaCMS access to ensure access is justified and approved.

DMAS will develop internal procedures to grant and review access in accordance with VaCMS access policies and procedures to ensure it properly assigns and controls access.

Currently, DMAS Security (OCS) contacts DSS Security, immediately if a problem is discovered, in order to address the issue directly, rather than delay making the problem worse. DMAS watches DSS SPARK website, for changes affecting DMAS VaCMS users.

Responsible Persons:

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

Estimated Implementation Date: March 31, 2017

Continue Improving Accounts Receivable Collection Process (issued as MP#9)

Condition

Medical Assistance Services Fiscal Division is not pursuing collections from providers and recipients timely and in accordance with its policies and procedures. In the cases reviewed from each Program Integrity Unit, Medical Assistance Services' actions have resulted in a delay of possible collections.

Of the 25 Recipient Audit Unit cases reviewed, we found the following:

- Two cases where invoicing letters were not sent timely.
- Six cases where the follow-up collection steps were not completed.
- Two cases that were referred to the Virginia Office of the Attorney General for collection. However, there was no supporting documentation of the referral.
- Two cases where repayment plans were established. However, repayments did not occur, and management did not pursue collection.

Of the five Prior Authorization and Utilization Review (PAUR) mental health provider cases reviewed, we found the following:

- One case where management was not able to provide any documentation to show that collection efforts were made.
- One case where neither a revised payment plan nor a negative balance was established.

Of the eight PAUR hospital provider cases reviewed, we found the following:

- One case where invoicing letters were not sent timely.
- Two cases where negative balances were not established timely.

Of the eight Provider Review Unit cases reviewed, we found the following:

- One case where the follow-up collection steps were not completed.

Recommendation

Medical Assistance Services should continue to 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.

Corrective Action Plan:

DMAS will continue to pursue improvements in the Accounts Receivable (AR) collections process by developing and implementing automated processing functions. This transition to automated processing functions has been delayed by a shift in priorities to the replacement of the financial system and the MMIS.

To date, the Fiscal AR Unit has implemented a process for scanning overpayment documents and storing them electronically. This new process has eliminated the need for paper folders. This improvement will ensure that documentation for all cases is available and accessible, and it will eliminate the risk of losing paper copies of cases. This improvement has already been implemented for all new cases. Old case files that were established prior to this date will remain in paper files until they are closed.

The Fiscal Division is working to implement a process that will automatically generate receivables and letters at the required intervals. This new process requires that an Excel spreadsheet template accompany all new receivable cases. The spreadsheet template will be completed by the entity conducting the audit (usually, this is the Program Integrity Division or audit contractors) and forwarded to the Fiscal Division with the original overpayment letter. The Fiscal Division will upload the spreadsheet to an Oracle staging area. The spreadsheet will trigger Oracle to set-up a receivable, generate letters, and electronically save the letters at the required intervals. This new automated process will reduce the amount of manual work required to work receivable cases and alleviate the need for additional staff.

Additionally, this process will automatically alert the Fiscal Division to refer cases the Division of Debt Collection of the Office of Attorney General (OAG), or a collection agency based on invoice date and status. These cases are sent to the OAG and collection agency quarterly. Full negative balances in MMIS and repayment agreements are reviewed monthly to determine if they need to be moved to the next step in the process.

This process should be complete and operational by April 30, 2017 for provider receivables. It is expected that implementing this same process for recipient receivables will take longer because they are more complex; the process for recipient receivables is expected to be complete and operational by June 30, 2017.

Responsible Persons:

- Karen Stephenson, Controller, DMAS Fiscal and Purchases Division

Estimated Implementation Date: The estimated completion date for the provider receivable is April 30, 2017 and June 30, 2017 for the recipient receivables.

The completion date of this automation project has already been delayed by the financial system and MMIS RFP. Some risk of further delay may exist due to the pending upgrade of the financial system. Meeting the deadlines may be impacted by our ability to make the needed changes to Oracle Financials as any new changes require approval from management due to the pending upgrade of Oracle to R12.

AGENCY OFFICIALS

As of June 30, 2016

Department of Medical Assistance Services

Cynthia B. Jones – Director

Department of Social Services

Margaret R. Schultze – Commissioner

Department of Behavioral Health and Developmental Services

Jack Barber, M.D. – Interim Commissioner

Department of Health

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