



AGENCIES OF THE SECRETARY OF HEALTH AND HUMAN RESOURCES

REPORT ON AUDIT FOR THE PERIOD ENDING JUNE 30, 2014

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





Martha S. Mavredes, CPA

Report Highlights

Audit of the Agencies of the Secretary of Health and Human Resources – For the Year Ending June 30, 2014

January 2015

Summary of Audit Results

During our audit, we found the following:

- Proper recording and reporting of transactions, in all material respects, in the Commonwealth Accounting and Reporting System and in each agency's accounting records;
- Six matters that we consider to be **material weaknesses** in internal controls;
- Thirty-eight additional matters that we consider to be **significant deficiencies** in internal control; and
- Instances of noncompliance with applicable laws and regulations that are required to be reported under Government Auditing Standards.

Summary of Selected Issues and Recommendations

[6] findings for the **Special Supplemental Nutrition Program for Women, Infants, and Children (WIC)** Program collectively prevented us from obtaining sufficient appropriate audit evidence to support an unmodified opinion on compliance. Many of these are findings resulting from issues encountered during the implementation of a new benefits system, Crossroads. The **Virginia Information Technologies Agency (VITA)** and the **Office of the Secretary of Health and Human Resources** may want to monitor Health's progress in addressing these issues and determine if there are any lessons that can be learned from this implementation that can be applied in the future.

[1] risk alert related to the Commonwealth of Virginia's compliance with its **settlement agreement with the United States Department of Justice (DOJ)**. The settlement is an agreement to address concerns with services provided by the Department of Behavioral Health and Developmental Services (DBHDS). We encourage **DBHDS**, the **General Assembly**, and the **Administration** to work together to ensure that Behavioral Health has the funds and support it needs to continue to comply with the settlement agreement and provide services to individuals in the appropriate setting.

[10] findings related to Information System User Access. These findings are related to information system owners improperly managing the access that users have to their critical systems. These findings should be of concern to the **Virginia Information Technologies Agency (VITA)** and the **Department of Accounts**, as they are responsible for issuing guidance in these areas. Many of the affected systems feed financial information directly into the Commonwealth's CAFR issued by the **Comptroller**.

[11] additional findings are related to Federal Compliance. These findings cite **specific compliance violations** with the Code of Federal Regulations or the Federal Office of Management and Budget (OMB) Circulars. Federal compliance findings could result in questioned costs, and liabilities to the federal government if corrective actions are not taken by management. These issues may require additional resources and supervision in order to correct; and therefore, should be monitored by management.

Why the APA Audits These Five Agencies Every Year

Collectively the following five agencies spent \$12 billion, or 97%, of the total funds expended by the **Agencies under the Secretary of Health and Human Resources**:

- **Department of Medical Assistance Services;**
- **Department of Social Services;**
- **Department of Behavioral Health and Developmental Services;**
- **Department of Health; and**
- **Office of Comprehensive Services for At-Risk Youth and Families**

As a result, these five agencies are material to the **Comprehensive Annual Financial Report (CAFR)** of the Commonwealth. Therefore, we are required to audit their financial activities in support of our audit opinion on the CAFR. Additionally, the federal government required us to audit eight federally supported programs for compliance in fiscal year 2014. We reviewed the controls and audited compliance for these programs in support of the **Commonwealth's Single Audit**.



See the full report at
www.apa.virginia.gov

101 N 14th Street, Richmond, VA 23219
(804) 225.3350

– TABLE OF CONTENTS –

	<u>Pages</u>
EXECUTIVE SUMMARY	
DEPARTMENT OF HEALTH	1-26
Improve Access Controls for the Crossroads System	1
Account for All WIC EBT Food Instruments and Investigate Errors	2
Record Accurate Time and Effort Reporting	4
Complete Local Agency Monitoring Reviews	5
Submit Invoices for WIC Rebates and Medicaid Claims	6
Improve Controls over Federal Reporting WIC – Repeat	7
Improve Procurement Controls	8
Improve User Access Controls for ROAP System – Repeat	10
Improve Controls over Federal Reporting – Repeat	11
Improve Internal Controls over the ROAP System Reconciliation Process for CACFP	12
Review Subrecipient Single Audit Reports and Issue Management Decisions – Repeat	13
Complete Subrecipient Monitoring Reviews – Repeat	14
Complete FFATA Reporting for CACFP – Repeat	15
Improve Database Security – Repeat	16
Improve Access Management to Information Systems	16
Ensure Timely Security Awareness and Training	17
Improve VNAV Reconciliation and Confirmation Process	19
Enforce Business Rules in Human Resource Transactions	20
Improve Documentation to Support Salary Changes	21
Improve Controls over Human Resources Transactions	22
Improve Controls over Reporting Account Receivables	24
Complete FFATA Reporting for Preparedness Grants	26
DEPARTMENT OF BEHAVIORAL HEALTH AND DEVELOPMENTAL SERVICES	27-39
Continue to Comply with the DOJ Settlement Agreement – Risk Alert	27
Improve Database Security – Repeat	28
Improve IDOLS Security	29

Develop and Submit an Information Technology Audit Plan	29
Improve Controls over Systems Access – Repeat	30
Improve Controls over Hours Worked by Wage Employees	32
Improve Controls over the VNAV System	34
Improve Controls over Payroll	36
Improve Controls over Physical Inventory	38
Create Policies and Procedures for Fixed Assets	39
DEPARTMENT OF MEDICAL ASSISTANCE SERVICES	40-48
Improve Access Reviews of the Medicaid Management Information System – Repeat	40
Create Formal Documentation that Facilitates Controlling Privileges in the Medicaid Management Information System	41
Identify a Back-up for Medicaid Management Information System Administration and Document the Process	42
Correct Operating Environment and Security Issues Identified by their Security Compliance Audit	43
Strengthen Financial System Application Access	45
Confirm that Application Access is Appropriate	47
Rates Used by the System Should be Supported by a Signed Contract with the Same Rates	48
DEPARTMENT OF SOCIAL SERVICES	49-55
Document IT Systems Backup and Restoration Policy and Procedure	49
Monitor Actions of Employees Granted Temporary Access in FAAS	50
Ensure Compliance with the Federal Funding Accountability and Transparency Act	51
Review User Accounts and Privileges for Mission Critical Systems – Repeat	52
Develop Workable Solutions to Maintain Appropriate Balance of Internal Controls – Repeat	53
Implement and Monitor a Change Management Process for Sensitive Applications – Repeat	55
INDEPENDENT AUDITOR’S REPORT	56-60
AGENCY RESPONSES	61-77
AGENCY OFFICIALS	78

Why the APA Audits the Special Supplemental Nutrition Program for Women, Infants, and Children

The Special Supplemental Nutrition Program for Women, Infants, and Children (WIC) represents approximately \$97 million in annual federal expenditures in the Commonwealth that support the health of pregnant women, infants and children through better nutrition and access to health care. The Department of Health (Health) is the Commonwealth's administrator of the WIC program, and is responsible for ensuring compliance with all federal regulations. During fiscal year 2014, Health implemented Crossroads, an information management system that Health is using to manage grant compliance for the WIC program.

We compared various aspects of the WIC program to federal regulations in the areas of allowable costs, time and effort reporting, participant eligibility, program income, procurement standards, monitoring, and reporting. We also evaluated system access and controls for the Crossroads system and compared their practices to the Commonwealth's Information Security Standard. Our testwork for the WIC program resulted in the following seven recommendations and a qualified opinion on the WIC program as further described in the Independent Auditor's Reports included in the Statewide Single Audit.

Improve Access Controls for the Crossroads System

Condition

Health is not properly managing administrator access to the Crossroads application. The Crossroads system is a web-based application that acts as the system of record for the CFDA #10.557 Special Supplemental Nutrition Program for Women, Infants, and Children (WIC). We identified system administrator accounts that are not being monitored appropriately. The accounts were assigned to the system's development contractor, but were assigned to individuals that are either no longer employed with the contractor or no longer assigned to work on the project for Health.

Criteria

The Commonwealth's Information Security Standard, SEC 501-08 (Security Standard) requires a formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and formal, documented procedures to facilitate the implementation of the access control policy and associated access controls. Additionally, each agency shall or shall require that its service provider document and implement account management practices for requesting, granting, administering, and terminating accounts.

Consequence

Untimely removal of access has resulted in unauthorized access to the Crossroads application through the administrator accounts assigned to the separated contractors. The accounts are being accessed after the separation date of the contracted employee, and their activities within the system are not being reviewed by Health. The accounts can be used for unauthorized activities or are being shared with other users. Since no review has taken place and there is no evidence of who is using these accounts, management cannot assure itself that unauthorized or fraudulent transactions did not take place.

Cause

Although Health monitors its own employees' access monthly, the developer's administrator accounts were specifically excluded from the review. Health has no process to remove the user accounts for these contractors timely, even though the contractor communicated that the employees were no longer working on the Crossroads project.

In some cases, the contractors' Commonwealth of Virginia (COV) accounts with the Virginia Information Technologies Agency were terminated, but their access to Crossroads was not terminated. Due to the nature of the contractors' accounts in Crossroads, the deletion of the COV account did not prevent access to the Crossroads system.

Recommendation

Health should consider all accounts, including those of contractors, in system access reviews for all systems. Health should also consider requiring all system contractors to maintain a COV network account in order to access the Crossroads system, and link their Crossroads account to the active COV network account. Health should also prohibit the use of shared accounts on all information technology (IT) systems. In addition Health should implement a method for reviewing the activities of contractors with administrator access.

Account for All WIC EBT Food Instruments and Investigate Errors*Condition*

Health is not properly accounting for the disposition of all issued food benefits for the CFDA #10.557 Special Supplemental Nutrition Program for Women, Infants, and Children (WIC). The eWIC Electronic Benefit Transfer (EBT) system processes the redemption of food benefits by WIC participants at retailers. After redemption, the details of the transactions are transmitted to the Crossroads grant management system, where the redemptions are matched with benefits that were validly issued by Health. Some of the redemptions that are being transmitted to Crossroads are not being imported properly; therefore, they are not being matched with valid benefit issuances. According to Health, due to the volume of these issues, which represent approximately \$92,000, Health is not currently investigating the individual non-imported transactions. However, Health is still paying the EBT vendor for these transactions.

In order to increase our assurance that these non-reconciling transactions represented valid and allowable benefit issuances, we attempted to obtain a Service Organization Control (SOC) report related to Health's EBT vendor. SOC reports are a type of internal control report that describe the suitability, design, and effectiveness of internal controls that are used at an outsourced service provider. Health relies on its EBT vendor to enforce certain critical controls for the WIC program; however, Health did not have an appropriate SOC report available.

Criteria

According to 7 CFR §246.19(q) Health must account for the disposition of all food instruments and cash-value vouchers as either issued or voided, and as either redeemed or unredeemed. Redeemed food instruments and cash-value vouchers must be identified as validly issued, lost, stolen, expired, duplicate, or not matching valid enrollment and issuance records. In an EBT system, evidence of matching redeemed food instruments to valid enrollment and issuance records may be

satisfied through the linking of the Primary Account Number associated with the electronic transaction to valid enrollment and issuance records. This process must be performed within 120 days of the first valid date for participant use of the food instruments

Additionally, 7 CFR §246(k) requires Health to design and implement a system to review food instruments and cash-value vouchers submitted by vendors for redemption to ensure compliance with the applicable price limitations and to detect questionable food instruments or cash-value vouchers, suspected vendor overcharges, and other errors. Health must take follow-up action within 120 days of detecting any questionable food instruments or cash-value vouchers, suspected vendor overcharges, and other errors and must implement procedures to reduce the number of errors when possible.

Consequence

The redemptions that are paid from the eWIC EBT system that cannot be matched with a valid benefit issuance in the Crossroads system create a reconciling difference between the two systems. Health continues to pay their EBT vendor the full amount of the reported redemptions, even if the amount is not reconciled to a valid benefit issuance in Crossroads. If these redemptions are not ultimately determined to be valid, then the costs are unallowable to the WIC program.

According to 7 CFR §246.23, Food and Nutrition Services (FNS) will establish a claim against any state agency that has not accounted for the disposition of all redeemed food instruments and cash-value vouchers and taken appropriate follow-up action on all redeemed food instruments and cash-value vouchers that cannot be matched against valid enrollment and issuance records, including cases that may involve fraud, unless the state agency has demonstrated to the satisfaction of FNS that it has:

- (i) Made every reasonable effort to comply with this requirement;
- (ii) Identified the reasons for its inability to account for the disposition of each redeemed food instrument or cash-value voucher; and
- (iii) Provided assurances that, to the extent considered necessary by FNS, it will take appropriate actions to improve its procedures.

Cause

During fiscal year 2014, Health implemented a new system for managing WIC benefits (Crossroads) and transitioned from paper checks to electronic benefits. According to Health, there are known issues with communication and reconciliation between Crossroads and the eWIC EBT system, some of which have existed since user acceptance testing in fall 2013. Health believes the non-reconciling items are caused by problems with invalid product codes and data loss due to a known service disruption in May 2014. According to Health, they are currently working with their system developers on a system modification that should resolve these issues.

Recommendation

We recommend that Health continue to work with their system developers and test the proposed system modifications that will allow for a complete reconciliation of issued and redeemed

benefits. Additionally, Health should investigate all remaining questionable redemptions of benefits, and any benefits that cannot be matched with valid issuance records.

Health should also work with the EBT vendor to obtain an SOC report in order to ensure that the controls Health is relying on are working as intended.

Record Accurate Time and Effort Reporting

Condition

Employees in the Office of Family Health Services (OFHS) at Health did not accurately record their time and effort reporting. Time and effort reporting determines the amount of personal service costs that are billed to federal awards. CFDA #10.557 Special Supplemental Nutritional Program for Women, Infants, and Children (WIC) was billed for \$20,481,399 in personal services costs during our audit period. Instead of reporting time and effort according to the actual activity of each employee, Health employees reported their time each pay period according to an estimate that was determined before the activity was performed.

Criteria

According to OMB Circular A-87, where employees work on multiple activities or cost objectives, a distribution of their salaries or wages will be supported by personnel activity reports. Personal activity reports must meet the following standards:

- (a) They must reflect an after the fact distribution of the actual activity of each employee,
- (b) They must account for the total activity for which each employee is compensated,
- (c) They must be prepared at least monthly and must coincide with one or more pay periods, and
- (d) They must be signed by the employee.
- (e) Budget estimates or other distribution percentages determined before the services are performed do not qualify as support for charges to federal awards.

Consequence

Health's time and effort documentation does not meet federal requirements for supporting charges to the WIC grant.

Cause

Employees were not properly trained on federal time and effort reporting requirements. Employees, including managers in OFHS, improperly reported and subsequently approved time and effort reporting that was not an after the fact distribution of the actual activity of each employee.

Recommendation

According to Health, after a review by the Food and Nutrition Service in June 2014, OFHS management conducted time and effort training sessions in which employees have been instructed that they are to record their hours in the Time and Effort system based on their actual work output. Health should continue to monitor the implementation of their corrective actions provided to the Food and Nutrition Service and ensure the ongoing accuracy of time and effort reporting.

Complete Local Agency Monitoring Reviews*Condition*

Health did not complete any on-site monitoring reviews in federal fiscal year 2014 for CFDA #10.557 Special Supplemental Nutrition Program for Women, Infants and Children (WIC). Health did not complete reviews for any of the 35 local health agencies. Local health departments, with the exception of Fairfax and Arlington, are not “local agencies” according strictly to the definition in 7 CFR §246; they are organizational units of Health. Health did perform a review of Fairfax in fiscal year 2013; therefore, only Alexandria was not reviewed timely per federal regulations. However, Health’s decision to forgo on-site reviews of the remaining organizational units did not properly consider the impact on internal controls throughout the agency because these on-site reviews are used as a critical tool to ensure many of the controls are working as intended.

Criteria

According to 7 CFR §246.19 the state agency shall conduct monitoring reviews of each local agency at least once every two years. Such reviews shall include on-site reviews of a minimum of 20 percent of the clinics in each local agency or one clinic, whichever is greater. Monitoring of local agencies must encompass evaluation of management, certification, nutrition education, breastfeeding promotion and support, participant services, civil rights compliance, accountability, financial management systems, and food delivery systems. If the state agency delegates the signing of vendor agreements, vendor training, or vendor monitoring to a local agency, it must evaluate the local agency’s effectiveness in carrying out these responsibilities.

Consequence

Insufficient monitoring by Health increases the risk of program non-compliance at the local agency level. Additionally, with the implementation of the new Crossroads WIC management system, there is increased risk of program non-compliance. The Commonwealth, through Health, is liable to the federal government for any funds not used according to program regulations.

Cause

Due to the implementation of the new Crossroads grant management system, management at Health made a decision not to perform any official on-site monitoring visits during the fiscal year. Health's management believed that scheduled on-site training for the Crossroads system was an adequate compensating control. However, the training visits did not satisfy the monitoring requirements described above. Health's management has stated that their grantor, the United States Department of Agriculture (USDA) approved of this decision. However, at the time of our audit, Health was unable to provide evidence that demonstrated explicit approval from USDA that allowed non-compliance with federal regulations.

Recommendation

Health should complete on-site reviews of local agencies every two years as required by federal regulations. Health should also implement internal controls to ensure that these reviews are completed timely, and in compliance with federal monitoring standards as described in 7 CFR §246.19.

Submit Invoices for WIC Rebates and Medicaid Claims*Condition*

Health did not submit approximately \$5.1 million in infant formula rebates and Medicaid claims for the CFDA #10.557 Special Supplemental Nutrition Program for Women, Infants, and Children (WIC) during the state fiscal year. Health has rebate contracts with the manufacturers of infant formula used in the WIC program. The income from these contracts is used to offset food expenditures incurred by the program. Additionally, WIC has an agreement with the Virginia Department of Medical Assistance Services that allows WIC to be reimbursed for certain formula purchases made by WIC participants that are dual-eligible for Medicaid and WIC programs.

Criteria

According to 7 CFR §246.10, at a minimum, a WIC state agency must coordinate with the State Medicaid Program for the provision of exempt infant formulas and WIC-eligible nutritionals that are authorized or could be authorized under the State Medicaid Program for reimbursement and that are prescribed for WIC participants who are also Medicaid recipients. Additionally, 7 CFR §246.16a requires all state agencies to continuously operate a cost containment system for infant formula.

Consequence

By not submitting the invoices for rebates and Medicaid claims, the WIC program required more federal funds for operation than necessary, had these cost containment practices been executed timely. According to 7 CFR §246, any state agency that Food and Nutrition Services (FNS) determines to be out of compliance with the cost containment requirements for the WIC program must not draw down on or obligate any program grant funds, nor will FNS make any further program funds available to such state agency, until it is in compliance with these requirements.

According to Health, the issue with infant formula rebates is now corrected, and the unbilled portions have been recovered, resulting in no permanent financial loss. However, Health only has up to one year to submit their Medicaid claims and will suffer financially if this capability does not exist by the end of November 2014.

Cause

The infant formula rebates and Medicaid claims were not submitted because of known issues with the implementation of the new Crossroads system beginning with the Crossroads pilot in November 2013 and regional roll-out beginning in March 2014. According to management at Health, these issues were communicated to the United States Department of Agriculture (USDA), their grantor, prior to and during the implementation of Crossroads. Per Health, USDA did not see this lack of functionality as a critical issue due to the availability of funding for WIC food costs and their confidence that these issues would be addressed.

Recommendation

According to Health, the formula rebate process is now functioning as designed. Health should ensure that the timely billing of these formula rebates continues as required. Health should work with the appropriate parties in order to fix the Medicaid claims billing process. If the inability to bill these claims results in a loss of income to the program, Health should work with their grantor, the USDA, to determine the appropriate recourse.

Improve Controls over Federal Reporting WIC – Repeat

Condition

Health does not have adequate controls in place to ensure accurate federal reporting on the FNS-798 financial and participation report for the CFDA #10.557 Supplemental Nutrition Program for Women, Infants, and Children (WIC). The participation data changed multiple times during our testwork as Health gained a better understanding of the Crossroads electronic benefits system, implemented in November 2013. Health made adjustments of approximately \$1.6 million to the FNS-798 during the fiscal year because the Crossroads system was over reporting actual food expenditures due to a system flaw that was discovered after several months. Additionally, supporting documentation could not be provided for multiple reported items, including the amount spent on breast pumps, number of participants in the program, and food expenditures.

Criteria

7 CFR §246.25 subparts (b) and (d) state the following related to the monthly 798 report and source documentation:

b.) Financial and participation reports—(1) Monthly reports. (i) State agencies must submit financial and program performance data on a monthly basis, as specified by Food and Nutrition Services (FNS), to support program management and funding decisions. Such information must include, but may not be limited to:

(A) Actual and projected participation;

- (B) Actual and projected food funds expenditures;
 - (C) Actual and projected rebate payments received from manufacturers;
 - (D) A listing by source year of food and NSA funds available for expenditure; and,
 - (E) NSA expenditures and unliquidated obligations.
- d.) Source Documentation: To be acceptable for audit purposes, all financial and Program performance reports shall be traceable to source documentation.

Consequence

FNS uses the reports to assess the state’s progress in achieving the objectives of the WIC program. Inaccurate financial and participation information provided to FNS limits their ability to monitor the program. Additionally, multiple resubmissions of federal reporting require the unnecessary use of administrative time.

Cause

Health implemented the Crossroads electronic benefits system for the WIC program during fiscal year 2014. Several components of the reporting system were not functional for most of the fiscal year. This includes some of the reports that are required to create the FNS-798, and a dedicated reporting server that will provide the users with a reliable reporting environment. Additionally, Health had to combine financial and participation data from their legacy WICnet system with data from the new Crossroads system in order to submit accurate reporting.

As a result, Health created ad hoc reporting tools as a substitute, in order to report information to FNS timely. However, due to Health’s unfamiliarity with their new Crossroads system, unavailable information that linked participants between the two systems, and a lack of documented policies and procedures, there have been several revisions to the FNS-798 report.

Health has also identified an issue that prevents accurate reporting of participation data from the Crossroads system within the timeframe required by FNS. According to Health, they have submitted a change request to the Crossroads developers in order to resolve this issue.

Recommendation

Health should continue to gain a better understanding of the Crossroads reporting function and work with their developers to ensure actual participation data can be reported timely. Ultimately, Health should work with their developers to ensure that Crossroads’ native application reporting function is operating as required by their contract. Additionally, Health should implement policies and procedures over the reporting process to ensure accurate and timely reporting of both participation and financial information to FNS.

Improve Procurement Controls

Condition

Our review of procurement transactions charged to CFDA #10.557 Special Supplemental Nutrition Program for Women, Infants and Children (WIC) identified several items that we consider

to be non-compliant with the Commonwealth's procurement policies. The noncompliance issues related to insufficient documentation in support of procurement decisions and purchased services over \$5,000 in which bids were not solicited.

Criteria

States, and governmental subrecipients of states, will use the same state policies and procedures used for procurements from non-federal funds. The Commonwealth's policies and procedures governing procurement are contained in the Virginia Department of General Services' (DGS) Agency Procurement and Surplus Property Manual (APSPM).

Consequence

The APSPM is designed to ensure that public bodies in the Commonwealth obtain high quality goods and services at reasonable cost, that all procurement procedures are conducted in a fair and impartial manner with avoidance of any impropriety or appearance of impropriety, and that all qualified vendors have access to public business and that no offeror be arbitrarily or capriciously excluded. Non-compliance could result in the failure of those objectives, and in the case of federal awards, questioned or potentially unallowable costs can be incurred.

Cause

Health failed to maintain evidence that demonstrated a consistent application of procurement standards as required by the APSPM. Inadequate recordkeeping in support of proprietary product purchases, proposal evaluations, and rental contracts reduced the auditable trail that is necessary to understand the why, who, what, when, where, and how of each transaction. Additionally, Health did not properly monitor the expenditure amount of their service contract that should have been submitted for bids.

Recommendation

Health should improve controls over their procurement process that ensure procurement actions are in compliance with the APSPM. Specifically, Health should ensure that documentation in support of procurement decisions is maintained, and that bids and quotes are solicited for services that exceed \$5,000.

Why the APA Audits the Child and Adult Care Feeding Program

The Child and Adult Care Feeding Program (CACFP) provides \$43 million in assistance to lower income participants in eligible child care, family day care, Head Start, at-risk after school care, emergency shelter and adult care centers. Health administers this program for the Commonwealth, and is responsible for ensuring compliance with USDA's regulations for the program. Health uses the Regional Office Administered Program (ROAP) information system to manage eligibility records and compliance. We evaluated Health's monitoring of the non-profit organizations that are paid to administer the program locally, program expenditures, reporting of program results to United States Department of Agriculture (USDA), and other areas of compliance. We also evaluated Health's use of the ROAP system against the Commonwealth's own Information Security Standard. Our testwork related to CACFP resulted in the following six recommendations to management.

Improve User Access Controls for ROAP System – Repeat

Condition

Health is not adequately managing access to their Regional Office Administered Program (ROAP) system used to submit claims for reimbursement for the CFDA #10.558 Child and Adult Care Feeding Program (CACFP). Currently, Health does not obtain the termination of access request forms for employees who have separated from the agency, and does not terminate access for separated users timely. Health uses a spreadsheet user log as a master list of users to ROAP. This log does not contain all end users and does not have the correct level of permission documented for some users.

Criteria

Commonwealth's Information Security Standard, SEC 501-08 (Security Standard), AC-2 and AC-2-COV Account Management, detail the need for managing information system accounts. These standards include, but are not limited to, deactivating accounts of separated users in a timely manner and granting access to the system based on (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions.

Consequence

Monitoring system access with an inaccurate listing of system users impairs Health's ability to properly monitor user access, increasing the risk of unauthorized transactions within the ROAP system. ROAP is a web-based system, and terminated users can access the application from outside the agency after separation. Also, management does not perform a review of transactions in the system to ensure that separated employees are not engaging in unauthorized transactions.

Cause

Health has not fully complied with their corrective action plan formulated in response to the ROAP access finding in the prior year. User access management policies and processes remain insufficient to properly manage access to the ROAP system.

Recommendation

Health should implement user access controls to remove user access timely after separation or termination from the CACFP program. Health should also ensure that an accurate listing of user access is used when monitoring access.

Improve Controls over Federal Reporting – Repeat*Condition*

Health does not have sufficient controls in place to ensure accurate federal reporting for the CFDA #10.558 Child and Adult Care Feeding Program (CACFP). Health could not provide support for several of the expenditures related to the cost of food for participants reported on the quarterly or annual FNS-777 submitted to the United States Department of Agriculture (USDA). Furthermore, Health is unable to provide evidence that all federal reports are reviewed by management prior to submission, nor does Health have adequate policies and procedures to ensure ongoing reporting compliance.

Criteria

7 CFR §226.7 outlines Health's responsibilities for financial management, and line 13 of the FNS-777 report states, "I certify to the best of my knowledge and belief that this report is correct and complete and that all outlays and unliquidated obligations are for the purposes set forth in the award documents." By submitting and signing the report, Health is certifying that their report is complete and accurate. In addition, it is a management best practice to review all reports for accuracy before they are submitted to the federal government.

Consequence

USDA's Food and Nutrition Services uses the data captured by this report to monitor state agencies' program costs and cash draws. Incorrect data does not allow USDA to properly monitor Health and could lead to incorrect funding allocations from USDA. The lack of a review process increases the risk of inaccurate reporting due to human error. Inaccurate federal reports must be resubmitted, creating operational inefficiencies.

Cause

According to management, due to significant understaffing and high turnover within the Office of Family Health Services (OFHS) Division of Administration, supporting documentation for the reported expenditures on the FNS-777 and evidence of management review has not been retained. In addition, Health has no policies that outline how to complete the report or policies that require a review of federal reporting by management prior to submission.

Recommendation

For all amounts reported to the federal government, Health should maintain a full and complete auditable trail to supporting records. Additionally, Health should implement policies and

procedures over the reporting process to ensure continued compliance during staff transitions. These policies should require the review of federal reports by management prior to submission.

Improve Internal Controls over the ROAP System Reconciliation Process for CACFP

Condition

Health does not perform adequate reconciliations between their Finance and Administration (F&A) and the Regional Office Administered Program (ROAP) systems. Health uses the ROAP system to process claims for CFDA #10.558 Child and Adult Care Feeding Program (CACFP). The current reconciliations are performed with year-to-date data, and reconciling items identified during this process are not supported with documentation or corrected within ROAP. No procedures exist specific to the reconciliation of ROAP to F&A. Additionally, there is insufficient segregation of duties between the person who creates the list of payees in ROAP, transmits the list for payment, and reconciles the amounts paid between the two systems.

Criteria

The Office of Management and Budget's Circular A-133 §.300(c) requires auditees to maintain internal control over federal programs that provides reasonable assurance that the auditee is managing federal awards in compliance with laws, regulations, and the provisions of contracts or grant agreements that could have a material effect on each of its federal programs. Additionally, since Health uses claims information from the ROAP system as support for expenditures charged to federal grants, it is essential that transactions in the claims system are reconciled with actual transactions from the accounting system.

Consequence

Incorrect data within ROAP can lead to incorrect federal reports being submitted to the United States Department of Agriculture because many of the reports are generated directly from the system. Without adequate procedures governing the ROAP to F&A reconciliation, Health cannot ensure ongoing compliance and consistency during staffing changes. Furthermore, without adequate segregation of duties, Health is at an increased risk of unauthorized transactions. This risk is exacerbated by the lack of support maintained for reconciling items identified.

Cause

The claims module of ROAP suffers from a lack of comprehensive accounting and reconciliation documentation; therefore, the reconciliation to the agency's financial system is performed manually. Additionally, there were no written procedures in place during staffing turnovers within the Division of Administration that described the appropriate process required to complete the reconciliation, and how to address variances between the claims system and the accounting system.

Recommendation

Health should develop written procedures specific to performing the reconciliation between ROAP and F&A, which should include properly addressing reconciling items. As reconciling items are identified, the records should be adjusted in ROAP to reflect the payments made in F&A. Health

should also improve internal controls and segregations of duties to mitigate unauthorized transactions and ensure proper reconciliation between the two systems. Per management, Health is planning to replace the ROAP system. When procuring the new system, Health should consider including an automated reconciliation process as a required system feature.

Review Subrecipient Single Audit Reports and Issue Management Decisions – Repeat

Condition

Health is not reviewing single audit reports or issuing management decisions for subrecipients of the Child and Adult Care Feeding Program, CFDA #10.558. Health has developed policies and procedures to comply with monitoring requirements but has not fully implemented them yet.

Also, Health does not compare subrecipient audited Schedule of Expenditures of Federal Awards (SEFAs) to Health's internal accounting records to ensure the reasonableness of pass-through funds subject to audit.

Criteria

Office of Management and Budget (OMB) Circular A-133, Audits of States, Local Governments, and Non-Profit Organizations, Subpart D-Federal Agencies and Pass-Through Entities §__.400 Responsibilities, (d) Pass-through entity responsibilities, (4), (5), and (6), which are:

- (4) Ensure that subrecipients expending \$300,000 (\$500,000 for fiscal years ending after December 31, 2003) or more in federal awards during the subrecipient's fiscal year have met the audit requirements of this part for that fiscal year.
- (5) Issue a management decision on audit findings within six months after receipt of the subrecipient's audit report and ensure that the subrecipient takes appropriate and timely corrective action.
- (6) Consider whether subrecipient audits necessitate adjustment of the pass-through entity's own records.

Consequence

Insufficient review of single audit reports by Health increases the possibility of Health not detecting non-compliance or internal control issues at its subrecipients. Subrecipients that do not properly identify federal expenditures, or exclude amounts on their SEFA, increase the risk that Health cannot rely on the subrecipient single audit. Furthermore, failure to adequately review single audit reports prevents Health from knowing if a subrecipient's audit necessitates adjustments to Health's own records.

By Health not issuing management decisions on related audit findings, subrecipients may not know if their corrective actions are appropriate. In addition, some subrecipients may elect to not take corrective action without guidance from Health.

Cause

Due to staffing turnover, Health's implementation of new subrecipient monitoring policies and procedures developed in the prior year were not completed according to their intended schedule.

Recommendation

Health's management should designate staff to review subrecipient single audits and SEFAs to ensure compliance with OMB's Circular A-133 § .400(d)(4-6). Specifically, Health should ensure that necessary management decisions are delivered to subrecipients timely, and that subrecipient audited SEFAs are reasonable in relation to Health's records, in order to ensure proper audit coverage over pass-through funds.

Complete Subrecipient Monitoring Reviews – Repeat*Condition*

Health did not complete the minimum number of subrecipient monitoring reviews in federal fiscal year 2014 for the CFDA #10.558 Child and Adult Care Feeding Program (CACFP). Although Health reviewed 33.3 percent of its subrecipients, it failed to meet the requirement to review all sponsors once every three years. These reviews were missed due to an insufficient tracking process developed by Health to ensure compliance with federal monitoring regulations.

Criteria

United States Department of Agriculture (USDA) federal regulation 7 CFR §226.6(m) requires Health in each federal fiscal year to review 33.3 percent of all of its subrecipients as well as any subrecipients that have not been reviewed in the past three years. Per the USDA Monitoring Handbook for State Agencies: "The State agency should establish a system to schedule and track reviews to ensure it remains in compliance with the requirements. The State system should allow it to know at a glance, anytime during the review year, that it is meeting the number and type of reviews required or whether modifications need to be made in the schedule or caseload."

Consequence

Insufficient monitoring by Health increases the risk of program non-compliance at the subrecipient level. In addition, having an incomplete tracking document increases the possibility of missing reviews for the subrecipients not listed. This was confirmed when a sponsor was found to not have received a review in the past three years due to being excluded from Health's tracking tool. The Commonwealth, through Health, is liable to the federal government for any funds that program subrecipients do not use according to program regulations.

Cause

Health did not comply with their corrective action plan from the prior year of reconciling the subrecipient tracker semi-annually.

Recommendation

Health should improve their tracking process to ensure all subrecipients are reviewed on a three year basis according to grant requirements.

Complete FFATA Reporting for CACFP – Repeat

Condition

Health has not submitted timely Federal Funding Accountability and Transparency Act (FFATA) reporting for CDFA #10.558 Child and Adult Care Feeding Program (CACFP). The staff charged with completing the FFATA reporting did not retain adequate supporting documentation for batch uploads into the federal reporting system and misreported multiple subrecipients under the wrong Data Universal Numbering System (DUNS) number.

Criteria

FFATA and 2 CFR §170 require Health to submit FFATA reporting no later than the month following the month in which Health awards \$25,000 or more in federal funds to a subrecipient. The subawardee DUNS number is a key element required for compliance when completing FFATA reporting.

Consequence

Failure to comply with FFATA and corresponding regulations limits the federal government and taxpayers' ability to know which entities are receiving federal funds through Health.

Cause

According to management, due to significant understaffing and high turnover within the Office of Family Health Services (OFHS) Division of Administration, Health has been unable to complete the FFATA reporting.

Recommendation

Health should complete FFATA reporting as required. Management should also develop written procedures for the accounting staff to ensure continuing compliance during staffing changes.

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 within its systems. We compared Health's practices to those required by the Commonwealth Information Security Standard in the areas of database security, web application security, oversight of sensitive systems, and information system access. Our information system security testwork resulted in the following three recommendations to management.

Improve Database Security – Repeat*Condition*

Health continues not to implement certain controls in its database management system supporting the Regional Office Administered Program (ROAP) web application. During the fiscal year 2013 audit, we identified and communicated this weakness to management in a separate document marked Freedom of Information Act Exempt under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms. To date, this has not yet been resolved.

Criteria

The Commonwealth's Information Security Standard, SEC 501-08 (Security Standard), requires implementing specific controls to reduce unnecessary risk to data confidentiality, integrity, and availability.

Consequence

Health cannot ensure financial integrity for the ROAP system.

Cause

As reported in management's corrective action plans, the complete and proper solution to this prior finding is taking more than a year. We determined that Health contracted with the IT Partnership to remediate these concerns by November 30, 2014; further, we will continue to provide updates on this finding in future reports until management has had enough time to fully implement their corrective actions, and we have evaluated them for effectiveness.

Recommendation

We recognize that Health has made progress in resolving this weakness in accordance with their corrective action plan; therefore, we recommend Health continue to dedicate the necessary resources to implement the controls discussed in the communication marked FOIA-Exempt in accordance with the Security Standard.

Improve Access Management to Information Systems*Condition*

Health is not properly managing user access to the Personnel Management Information System, Commonwealth Integrated Payroll Personnel System, Health's internal Finance and

Accounting system, and WebVision, a system used to manage healthcare services at local health districts. Across these systems, we found a variety of issues in the proper granting of access, recordkeeping, timely termination of access for separated users, and in monitoring access to the systems on a regular basis.

Criteria

The Commonwealth's Information Security Standard, SEC 501-08 (Security Standard), requires a formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Consequence

Insufficient access management increases the risk of unauthorized access to agency systems, which could allow for improper transactions and unreasonable access to agency data.

Cause

The management of access to Health's information systems is highly decentralized, and the processes and policies surrounding access management vary between each business unit and system. Recordkeeping is also highly decentralized, and though system security guidance is provided by the central Office of Information Management, the business units also develop their own policies and processes for managing security to their applications.

The process for removing access to systems upon employee separation is also inconsistently applied across the agency. Some major systems are included on a checklist that is a part of the standard employee separation process managed by the Office of Human Resources, whereas other systems are not included. Our testwork indicates that the Office of Information Management does not have sufficient processes to manage access to all systems agency-wide, yet the business units do not have sufficient processes or training to manage access independently.

Recommendation

Health should perform an agency-wide risk assessment of its approach to managing access to its information systems. Health should then determine what additional controls, processes, and resources are required to mitigate the current risks. Health should then communicate these changes to all agency employees responsible for information system management, provide appropriate training, and monitor this implementation to ensure controls are working properly.

Ensure Timely Security Awareness and Training

Condition

Health does not disable user accounts for employees that do not attend Health's annual mandatory security awareness and training program. Further, approximately 16 percent of Health's employees did not complete this training in fiscal year 2014 and continued to have access to Health information systems.

Criteria

Health's policy and the Commonwealth's Information Security Standard, SEC 501-08 (Security Standard), Section 8.2: Awareness and Training, require Health to annually provide security awareness and training to all information system users, including employees and contractors.

Consequence

Without security awareness and training, Health increases the risk of a user making an inadvertent mistake that may potentially lead to incidents such as a data breach or system unavailability.

Cause

Health does not enforce its policy that requires employees to attend security awareness and training each year. Typically, this control is enforced by disabling the employees' user accounts until the employees have attended the annual security awareness and training program.

Recommendation

We recommend that Health disable user accounts that belong to employees who have not completed the annual security awareness and training program. We also recommend that Health maintain sufficient records of training completion in accordance with the Security Standard.

Why the APA Audits Payroll and Human Resources

Health spends approximately \$239 million, or 40% of its budget, on payroll and other personal service expenses. Due to the significance of this activity, we consider payroll and human resource controls to be critical. These controls ensure both the accuracy of payroll and compliance with state payroll requirements. We evaluated Health's practices against their own policies as well as the requirements set by Department of Accounts and Department of Human Resource Management. Our testwork resulted in the following four management recommendations.

Improve VNAV Reconciliation and Confirmation Process

Condition

Health does not have adequate controls in place to ensure that retirement information for employees is accurate. Specifically, Health is not reconciling their payroll system, the Commonwealth Integrated Personnel and Payroll System (CIPPS), to the Virginia Retirement System (VRS) MyVRS Navigator (VNAV) system which contains essential retirement data for state employees. Per VRS policy, Health must confirm the accuracy of the VNAV data monthly. In addition, Health is not reviewing the required error reports from the Personnel Management Information System (PMIS) before confirming that VNAV is accurate. In five out of the 12 months in the period under audit, these confirmations occurred after the deadline set by VRS. Finally, Health has not implemented adequate segregation of duties surrounding the confirmation process, as one person performs all tasks related to this process.

Criteria

Commonwealth policies (Commonwealth Accounting Policies and Procedures Manual Topic 50410) require each agency to reconcile VRS contributions monthly. The confirmation submitted by the agency as a result of their reconciliation efforts also asks them to verify that VRS has calculated the correct amount of retirement contribution for the agency's employees. Department of Accounts (Accounts) Payroll Bulletin Volume 2013-02 describes the due date for the Snapshot confirmations, review of the PMIS cancelled records report, and the VRS automated reconciliation reports.

Consequence

Because Health is not reconciling CIPPS and VNAV, individual employees' retirement calculations and contributions may be incorrect. Every month Accounts performs a high-level reconciliation of CIPPS and VNAV and then processes an interagency transfer for the difference between what Health confirmed in VNAV and the retirement contributions that were actually withheld and paid by the agency. Accounts cannot perform this reconciliation until all CIPPS agencies, such as Health, confirm their contributions. Health is receiving an overwhelming number of exceptions from this reconciliation and has not been able to clear all of the exceptions to date, leaving employees with possible overpayments or underpayments to the Virginia Retirement System. Beginning in fiscal year 2015, the Commonwealth will use the data in VNAV to calculate the Commonwealth's total pension liability so uncorrected errors could lead to inaccurate financial reporting in the Commonwealth's Comprehensive Annual Financial Report.

By not reviewing the PMIS Cancelled Records Report, Health is unaware when information does not transmit correctly between the human resource system (PMIS) and the retirement system (VNAV); and therefore, Health does not make appropriate corrections timely. This was confirmed when we identified an employee whose salary was keyed incorrectly into PMIS but correctly into CIPPS. As result of this error, her retirement contribution amount was being withheld based on incorrect information. This employee was found to be present on two different error reports since the start of her employment, yet the error remained uncorrected.

Cause

Health is in the process of implementing procedures to ensure the employee and contribution information in CIPPS, PMIS, and VNAV is accurate. However, due to minimal guidance from DOA and VRS, and insufficient staffing, Health has not completed their own reconciliation between CIPPS and VNAV, and has been unable to address the number of exceptions generated during the Accounts reconciliation process each month.

Recommendation

We recommend that Health put adequate controls in place to ensure that retirement information for employees is accurate. This should include ensuring CIPPS, PMIS, and VNAV are properly reconciled with one another, reviewing the PMIS cancelled records report, and clearing all exceptions before confirming the VNAV data monthly by the imposed deadline. Additionally, Health should ensure there is an adequate segregation of duties during the VNAV confirmation process.

Enforce Business Rules in Human Resource Transactions

Condition

In the period under review, 17 out of 269 human resources (HR) personnel transactions that required the approval of a Deputy Commissioner at the agency bypassed approval controls within Health's Finance and Accounting system (Web F&A). These transactions were related to temporary pay adjustments for staff, the removal of wage employees, and pre-disciplinary leave transactions.

Criteria

Health's own human resources policies outline the different types of HR transactions that require the approval of a Deputy Commissioner at the agency. These business rules are built into Health's HR Module of the Web F&A system, which is intended to enforce the business rules deemed critical by management. The Web F&A HR module was designed to capture all of the necessary approvals as dictated by policy.

Consequence

Transactions that do not receive the proper level of approval increase the risk of unreasonable transactions. It should be noted that these transactions were approved initially by a member of each respective work unit; however, the elevated approvals by Deputy Commissioners did not take place in the system. Health was able to provide hardcopy approvals for some of the transactions.

Cause

A defect in the Web F&A system is causing it to not properly enforce business rules that Health included in the system design.

Recommendation

Health's Office of Human Resources should work with the appropriate technical staff to correct the system malfunctions that are allowing transactions to bypass proper approvals. Until these system corrections are made, Health should develop a method to monitor for transactions that do not receive the proper approvals.

Improve Documentation to Support Salary Changes*Condition*

Health could not provide adequate documentation to support salary amounts reported for retirement contributions for two of the twenty-five employees tested. According to Health the two employees have not had any salary changes, other than statewide raises, since the current internal human resources system (Web F&A) was implemented; however, there was no evidence to support that the current salary amount was approved. Health did not retain consistent hardcopy documentation showing an auditable trail of approvals for these employees.

Criteria

Commonwealth Accounting Policies and Procedures Manual Topic 50135 states that agencies must ensure that documentation and authorization exists for all employee record changes and payroll transactions.

Department of Human Resource Management (DHRM) policy 6.10 defines the required documents for all personnel files including:

- 1) Originals of the Report of Appointment or Change of Status (P-3) and Personal, Faculty and Miscellaneous (P-3a) forms, or the official agency substitute forms, signed by appointing authorities.
- 2) Original agency personnel forms used to initiate personnel transactions.

Health developed Human Resources Policy 3.05 in response to DHRM's requirements, which states: "The rationale for each and every pay action is documented using a Pay Action Worksheet (PAW) form (HR5-PAW). The documentation must be sufficient that a third party, unfamiliar with the agency, would be able to understand the business need for the pay action and the rationale for the amount provided."

Consequence

Without documentation of approval of salary changes, current employee salaries cannot be supported.

Cause

According to Health, the policies and procedures concerning required documentation before Web F&A was implemented in 2010 were not consistently followed agency-wide.

Recommendation

Health should ensure for all employees that the current salary is supported by evidence of an approval. In addition Health should maintain documented support for all salary changes in order to ensure changes are appropriate and reasonable. This documentation should support an auditable trail of approvals such that a third party, unfamiliar with the agency, would be able to understand the business need for the pay action and the rationale for the amount provided.

Improve Controls over Human Resources Transactions*Condition*

Health does not have sufficient documentation to support numerous changes to positions that were made within the human resources (HR) system. In addition, the Office of Human Resources is unable to provide policies that outline the necessary approvals or recordkeeping requirements for the following transactions:

- Abolishing Position: this transaction eliminates a position at the agency (not necessarily an employee termination);
- Change Fund Source: these transactions determine the allocation of payroll costs for specific positions and employees; and
- Other transactions: these are transactions that change position supervisors, allow teleworking, and permit alternative work schedules.

During the audit period, 2,021 of the above positional transactions were processed by the HR system.

Criteria

The Comptroller's internal control standards require that agencies document, evaluate and test controls applicable to significant fiscal processes. Payroll accounts for over \$239 million in annual expenditures at Health; therefore, we consider the internal controls over these processes to be significant.

Consequence

Not having policies to outline the necessary approvals and recordkeeping requirements for position changes increases the risk that improper transactions can occur. Making changes to the fund source of a position or eliminating a position without retaining documentation to support the change increases the risk of budgeting errors or potential liabilities where Health could be liable to later repay costs associated with incorrectly allocated wages; for instance, an employee could be incorrectly billed to a federal award or another project with dedicated funding.

Cause

The Office of Human Resources does not maintain policies related to these transaction types, and delegates their responsibility to the individual work units at Health, however; the work units have not developed their own written policies for approval and recordkeeping in support of these transactions.

Recommendation

Health should perform an assessment of the HR position change process. Based on that assessment, Health should identify any and all risks, implement controls, and monitor their effectiveness. The Office of Human Resources should also consider developing policies or guidance for the work units, if the central Office of Human Resources does not intend on maintaining the policies and monitoring related to these transactions.

Why the APA Audits Financial Reporting

Health's financial activities are materially significant to the Commonwealth as a whole and as such have an effect on the Commonwealth's Comprehensive Annual Financial Report (CAFR). To ensure the CAFR is accurately represented, we reviewed all significant financial information submitted to the Department of Accounts to ensure it was accurate, complete, and in accordance with generally accepted accounting principles. Our testwork related to financial reporting resulted in the following finding.

Improve Controls over Reporting Account Receivables

Condition

Health understated their accounts receivable balance submitted to the Department of Accounts for inclusion in the Commonwealth's Comprehensive Annual Financial Report (CAFR) by \$5.1 million. This understatement was associated with CFDA #10.557, the Special Supplemental Nutrition Program for Women, Infants, and Children (WIC). Additionally, Health misclassified two other receivable amounts. These errors were corrected after we communicated them to management. Health's Office of Financial Management has central policies pertaining to the compilation of year end accounts receivable. However, several of the amounts reported are calculated and provided by different business units within Health. The decentralized business units do not have policies and procedures related to accounts receivable submissions. Further, the financial reporting preparation and review processes did not include sufficient procedures to prevent or detect these errors or omissions.

Criteria

Commonwealth Accounting Policies and Procedures Manual Topic 20505 states the following: "Agencies are responsible for developing systems that are adequate to properly account for and report their receivables, their age, collection status, and funding source to DOA quarterly." Health utilizes the fourth quarter receivables report to develop their receivables attachment for the CAFR.

Consequence

The accounts receivable balances reported by Health are incorporated into the Commonwealth's CAFR. Therefore, misstated amounts by Health would have led to misstated financial statements for the Commonwealth.

Cause

Due to issues with the implementation of a new WIC information system, Health was unable to accurately identify and report certain WIC rebates and did not initially accrue the receivable. Additionally, the Office of Financial Management did not communicate with the business units sufficiently to ensure an understanding of the use of the quarterly receivable balances once they are submitted.

Recommendation

Health should ensure all accounts receivable at year end are accurate and properly supported. In order to achieve this, Health should ensure their financial reporting procedures over accounts receivable provide sufficient direction for personnel in the business units regarding specifics on what should be reported, the support needed to prepare the submissions, as well as adequate controls to prevent or detect and correct mistakes, errors or omissions like those observed this year. Additionally, Health should improve their compilation and review process to ensure consistency among all business units.

Why the APA Audits Data Required by the Federal Funding Accountability and Transparency Act

Health awards federal funding to the Virginia Hospital and Healthcare Association in order to support emergency preparedness at hospitals and other healthcare facilities. The Federal Funding Accountability and Transparency Act requires that entities receiving federal funds report if those funds are disbursed to other entities. This allows citizens to see how their tax dollars are being spent, and provides a greater overall level of transparency for citizens. In order to determine compliance we compared Health's reporting with the requirements of this Act. This testwork resulted in the following recommendation to management.

Complete FFATA Reporting for Preparedness Grants*Condition*

Health's Office of Emergency Preparedness and Response has not correctly submitted Federal Funding Accountability and Transparency Act (FFATA) reporting for CFDA #93.074 Health Emergency Preparedness and Public Health Emergency Preparedness Aligned Cooperative Agreements. Currently Health has only submitted FFATA data through the month of August 2013.

Criteria

FFATA and 2 CFR §170 require Health to submit FFATA reporting no later than the month following the month in which Health awards \$25,000 or more in federal funds to a subrecipient.

Consequence

Failure to comply with FFATA limits the federal government and taxpayers' ability to know which entities are receiving federal funds through Health.

Cause

According to management, due to issues with incorrect Data Universal Numbering System (DUNS) numbers they are unable to complete FFATA reporting timely.

Recommendation

Health should complete FFATA reporting as required. Management should work with appropriate federal contacts to correct the DUNS number issues and ensure accurate and timely reporting.

Risk Alert – Continue to Comply with the DOJ Settlement Agreement

During the course of our audit, we encountered issues that are beyond the corrective action of the Department of Behavioral Health and Developmental Services (DBHDS) management and require the action and cooperation of management, the General Assembly, and the Administration. The following issue represents such a risk to DBHDS and the Commonwealth.

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 the Department of Justice and an independent reviewer to meet the terms of the settlement agreement, but there is 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. Specifically, funds are needed:

- to address critical and ongoing one-time requirements to build community capacity as well as remain compliant with other aspects of the settlement agreement;
- to support facility transition waiver slots to enable DBHDS to move individuals out of the training centers and into community based programs as well as additional community intellectual and developmental disability (ID/DD) waiver slots to help reduce the growing waiting list for services; and
- to maintain the certification staffing standards of training centers due to delays in the projected discharge of individuals into the community and/or the training centers remain open beyond their scheduled closure date due to unforeseen policy or operational considerations.

We 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 Information Systems Security

The Department of Behavioral Health and Developmental Services (DBHDS) collects, manages, and stores significant volumes of personal and financial data within its mission critical systems. Because of the highly sensitive and critical nature of this data, DBHDS management must take all necessary precautions to ensure the integrity and security of the data within its systems. To determine if 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 Standards.

Improve Database Security – Repeat

Condition

DBHDS continues to operate its databases that account for its financial activity without implementing the minimum controls in accordance with internal policy, the Commonwealth's Information Security Standard, and industry best practices. We communicated 13 areas of weakness during the fiscal year 2013 audit in detail to management in a separate document marked Freedom of Information Act Exempt under Section 2.2-3705.2 of the Code of Virginia, due to their sensitivity and description of security controls. Although these weaknesses are still not resolved, we recognize that DBHDS has made reasonable progress in resolving these weaknesses in accordance with their corrective action plan. DBHDS plans to have these control weaknesses remediated by November 2014.

Criteria

The Commonwealth's Information Security Standard, SEC 501-08 (Security Standard), requires implementing specific controls to reduce unnecessary risk to data confidentiality, integrity, and availability.

Consequence

DBHDS cannot ensure confidentiality, integrity, and availability for its financial database.

Cause

As reported in management's corrective action plans, the complete and proper solution to this prior finding is taking more than a year. We determined that DBHDS contracted with the IT Partnership to remediate these concerns by November 1, 2014; further, we will continue to provide updates on this finding in future reports until management has had enough time to fully implement their corrective actions, and we have evaluated them for effectiveness.

Recommendation

We recognize that DBHDS has made progress in resolving this weakness in accordance with their corrective action plan; therefore, we recommend that DBHDS continue to dedicate the

necessary resources to complete the SQL Server upgrade in accordance with the current Commonwealth's Information Security Standard and industry best practices, such as those published by the Center for Internet Security.

Improve IDOLS Security

Condition

DBHDS does not implement certain controls in its Intellectual Disability On-Line System (IDOLS) that contains protected health information. We identified and communicated two inadequate systems security controls to management in a separate document marked Freedom of Information Act Exempt under Section 2.2-3705.2 of the Code of Virginia due to it containing descriptions of security mechanisms.

Criteria

The Commonwealth's Information Security Standard, SEC 501-08 (Security Standard), requires implementing specific controls to reduce unnecessary risk to data confidentiality, integrity, and availability.

Consequence

DBHDS cannot ensure confidentiality, integrity, and availability for IDOLS.

Cause

DBHDS did not adequately manage or establish appropriate information security controls for IDOLS as management did not define its expectations through formal policies and procedures to appropriately configure IDOLS.

Recommendation

DBHDS should dedicate the necessary resources to implement the controls discussed in the communication marked FOIA-Exempt in accordance with the Security Standard.

Develop and Submit an Information Technology Audit Plan

Condition

DBHDS does not coordinate and plan audits over sensitive information technology (IT) systems to ensure they sufficiently protect data. DBHDS's Internal Audit Department has not developed or submitted an Information Technology Audit Plan for the past five years.

Criteria

The Commonwealth's Information Technology Security Audit Standard, SEC 502-02.2 Section 2.1, requires that agencies submit an IT audit plan to the Chief Information Security Officer (CISO) of the Commonwealth of Virginia on an annual basis. SEC 502-02.2 Sections 1.4 and 2.1 further require Commonwealth agencies to annually update and create a three-year IT audit plan that covers the

organization's sensitive IT systems. Additionally, the Commonwealth's standard requires that these audits are performed in accordance with either Government Auditing Standards (Yellow Book) or International Standards for the Professional Practice of Internal Auditing (IIA Standards). SEC 502-02 further requires at Section 2.2 that IT security audits be performed based on the minimum controls established in the Commonwealth's Information Security Standard, SEC 501-08 (Security Standard).

Consequence

IT system audits determine if reasonable controls are in place to protect sensitive data for each respective system. As DBHDS does not have a schedule for each sensitive IT system to be audited, DBHDS increases the risk of an IT system being overlooked that may contain significant risks that require remediation. These risks increase the risk of a potential data breach at DBHDS.

Cause

DBHDS Internal Audit did not establish an appropriate IT audit plan due to limited communication with management and a lack of understanding the SEC 502 requirements. Further, DBHDS management has not maintained an inventory of all sensitive IT systems that require audit.

Recommendation

DBHDS should establish a complete inventory of all sensitive systems. DBHDS should also dedicate the necessary resources to develop and submit timely annual three year IT audit plans to the Commonwealth CISO and complete them accordingly.

Improve Controls over Systems Access – Repeat

Condition

Individual facilities within DBHDS do not have adequate controls in place to ensure system access is appropriate in Kronos (HR and Payroll System), Personnel Management Information System (PMIS), Financial Management System (FMS), Lease Accounting System (LAS), Fixed Assets Accounting System (FAACS), AVATAR (state hospital database), and Commonwealth Accounting and Reporting System (CARS). Specifically:

- Five out of seven systems at nine facilities and the Central Office had employees whose access was not removed timely;
- Two out of seven systems at two facilities had missing and inaccurate user access forms for employee access; and
- Two out of seven systems at three facilities did not have user access forms with proper approval.

Criteria

The Commonwealth's Information Security Standard, SEC 501-08 (Security Standard), AC-2-COV, 2.e-h, requires the prompt removal of system access for terminated or transferred employees. The Security Standard AC-2-COV, 2 i, requires granting access to the system based on a valid access authorization. In addition, the Security Standard AC-2- COV, 2.c-d, requires appropriate approvals for requests to establish accounts.

Consequence

Untimely removal, missing and inaccurate forms, and missing approval of user access increases the risk of unauthorized individuals inappropriately entering or approving transactions and could affect the integrity of DBHDS transactions in the system.

Cause

DBHDS does not have adequate policies and procedures over granting, changing, and terminating system access. Specifically, policies and procedures lack the guidance on timeframes and contacts for removal of access.

Recommendation

Management should create, communicate, and implement policies and procedures over granting, changing, and terminating access for all systems at all DBHDS facilities and the Central Office.

Why the APA Audits Hours Worked by Wage Employees

The Department of Behavioral Health and Developmental Services (DBHDS) 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, DBHDS management must take all necessary precautions to prevent employees from exceeding allowable hours worked thresholds. To determine if the threshold was exceeded, we compared the hours worked by DBHDS wage employees to the hours allowed by the Virginia Acts of Assembly.

Improve Controls over Hours Worked by Wage Employees

Condition

Western State and Piedmont Geriatric Hospitals each had one wage employee that exceeded the allowable hours worked threshold for wage employees during the initial measurement period. Wage employees are not eligible to participate in the state health insurance plan.

Criteria

Chapter 806 of the 2013 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 Initial Standard Measurement Period as May 1, 2013, through April 30, 2014.

Consequence

Failure to comply with Chapter 806 of the 2013 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

A breakdown in monitoring processes at Western State and Piedmont Geriatric Hospitals resulted in two wage employees exceeding the allowable hours worked threshold. The hospitals identified the issue and prevented the two employees from working for the remainder of the measurement period, but not until after the employees exceeded the threshold.

Recommendation

Management should improve existing controls over monitoring of hours worked for wage employees to ensure that they do not exceed the allowable hours worked threshold. This should include identifying employees that could potentially exceed the threshold as they approach the threshold rather than after exceeding it.

Why the APA Audits Controls over the VNAV System

The Virginia Retirement System (VRS) has modernized the methods of collecting and reporting creditable compensation, service credit, and contributions for all participating employees. The implementation of the VNAV system shifted the responsibility of updating these records from VRS to the employers, to include the Department of Behavioral Health and Developmental Services (DBHDS). Because the records in VNAV are used to calculate total pension liabilities for the Commonwealth, DBHDS management must take all necessary precautions to ensure the integrity of these records. To determine if adequate precautions were taken, we compared the practices of DBHDS to the guidance provided by the Department of Accounts over the VRS billing process.

Improve Controls over the VNAV System

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:

- Seven of seventeen facilities did not perform contribution snapshots timely;
- Seven of seventeen facilities did not have documented policies and procedures to reconcile their payroll and human resource systems to the Virginia Retirement System's (VRS) VNAV system;
- Three employees in two facilities did not have access to the VNAV system that was appropriate for their job responsibilities; and
- Three instances of inadequate segregation of duties between the approval and payment functions exist in two facilities.

Criteria

Department of Accounts (Accounts) Payroll Bulletin Volume 2013-02 states that agencies must certify the Contributions Snapshot by the 10th 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 VNAV and the systems of record for payroll and human resources; to ensure that VNAV system access is both role based and centered on least privileges; and that proper segregation of duties is maintained.

Consequence

Untimely certification at the agency level impacts the ability of Accounts to process interagency transfers for any differences between the amounts confirmed in VNAV and the retirement contributions actually withheld and paid for all agencies across the Commonwealth. A lack of written policies and procedures at all DBHDS facilities provides insufficient guidance for employees to perform the reconciliations necessary to perform these certifications. Inappropriate

access to the VNAV system, whether through non-role-based privileges or improper segregation of duties, 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 VNAV to calculate the Commonwealth's pension liabilities and inaccurate data could lead to a misstatement in the Commonwealth's financial statements.

Cause

Staffing shortages, competing priorities, issues that required research, and the newness of this process at the local level contributed to the lack of timely certifications at all seven locations. The inappropriate access levels observed involved employees whose initial VNAV access provided them with the ability to schedule and approve payments of contributions following confirmation of the contribution snapshots; in all three instances, the facilities removed the access to both of these functions once we identified it. The inadequate segregation of duties involved payroll personnel approving VRS payments within the VNAV system.

Recommendation

Management should implement adequate controls and procedures at the facilities that consider staffing and other priorities to ensure timely performance of the monthly Contribution Snapshot. Management should also formally document policies and procedures necessary to perform the monthly reconciliations between the payroll, human resource, and VNAV systems at all facilities. Finally, management should ensure appropriate levels of VNAV system access, to include adequate segregation of duties, at all facilities.

Why the APA Works with DBHDS Internal Audit to Audit Payroll

The Department of Behavioral Health and Developmental Services (DBHDS) employs over 10,000 salaried and wage employees across 17 facilities. Because of the sizeable nature of this expense to the Commonwealth, DBHDS management must take all 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, resulting in the finding below.

Improve Controls over Payroll

Condition

Individual facilities within DBHDS do not have adequate controls in place to ensure Human Resources forms are completed and payroll is appropriate. Specifically:

- Twenty-three percent (28 out of 120) of the population tested at six out of six facilities tested did not have proper approval on payroll forms, overtime pay transactions, and pay changes, and
- Fifty percent (18 out of 36) of the population tested at four out of six facilities tested did not have a completed employee checkout checklist in the personnel file.

Criteria

Commonwealth Accounting Policies and Procedures(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. In addition, CAPP Manual Topic 50320 “Terminations” states agencies must verify that CIPPS information concerning terminating employees is complete, properly authorized, and entered accurately into the system and that all payments have been properly and accurately issued. The individual facilities payroll policies and procedures instruct the use of an employee checkout checklist as recommended by CAPP Manual Topic 50320.

Consequence

Not having proper approval of payroll forms, overtime pay, and pay changes increases the risk that DBHDS could pay unauthorized and incorrect salaries. Not completing the employee checkout checklist for terminated employees increases the risk that systems access is not removed, assets are not returned, credit cards are not canceled, and human resource forms are not completed.

Cause

These exceptions occurred because the individual facilities either did not comply with established CAPP manual guidance for payroll approvals or did not have documented local policies and procedures pertaining to employee terminations.

Recommendation

Management should evaluate and update policies and procedures to provide adequate guidance to ensure proper approval of payroll forms, salaries changes, and overtime. In addition, human resource and payroll personnel should receive proper approval for payroll forms and pay changes. Finally, human resource personnel should complete the employee checkout checklist when an employee is separating to ensure timely removal of systems access and proper accounting for all assets.

Why the APA Audits Fixed Assets Management

The Department of Behavioral Health and Developmental Services (DBHDS) has 17 individual locations throughout the Commonwealth. As part of its plan to comply with the Department of Justice settlement, DBHDS closed one facility in the current fiscal year and plans to close three additional facilities by the end of fiscal year 2020. Because of the large number of fixed assets associated with multiple locations, DBHDS management must take all 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 Commonwealth Accounting Policies and Procedures.

Improve Controls over Physical Inventory

Condition

Individual facilities within DBHDS do not have adequate controls in place to ensure physical inventory is properly performed, documented, and recorded in the Fixed Assets Accounting System (FAACS). Specifically:

- Three out of 17 facilities with fixed assets did not perform a physical inventory within the last two years. For one of these facilities, the last inventory count was in 2008; and
- One out of four facilities tested did not record the removal of five assets from FAACS timely. These assets were disposed in April, May, and June of 2013 but remain in FAACS as of December 2014.

Criteria

CAPP Manual Topic 30505 Physical Inventory states that a physical inventory of fixed assets is required at least once every two years in order to properly safeguard assets and maintain fiscal accountability. In addition, CAPP Manual Topic 30505 Physical Inventory requires the physical inventory must verify the asset's existence, and should provide a reference to lists and/or other documents evidencing the existence and cost of the asset examined. CAPP Manual Topic 30505 Physical Inventory further compels all asset transactions to be entered into FAACS in a timely manner.

Consequence

Improperly performing, documenting, or recording physical inventories increases the risk of loss or theft of fixed assets and inaccurate accounting of fixed assets.

Cause

DBHDS does not have adequate policies and procedures over the inventory of fixed assets.

Recommendation

Management should create, communicate, and implement policies and procedures over fixed asset inventories at all DBHDS facilities and the central office. In addition, management should perform a physical inventory at least once every two years and record any changes in FAACS timely.

Create Policies and Procedures for Fixed Assets

Condition

DBHDS lacks clearly documented and approved policies and procedures for fixed assets. The areas include but are not limited to:

- Fixed Assets Accounting System (FAACS)
- Physical Inventory
- Disposals
- Asset Depreciation
- Intangible Assets
- Capital Outlay
- Sales and Surplus of Land

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 control.

Consequence

The lack of fixed assets policies and procedures increases the risk of inaccurate accounting of fixed assets and contributed to the issues discussed in the finding "Improve Controls over Physical Inventory."

Cause

The individual facilities at DBHDS did not comply with established CAPP manual guidance to prepare and document in writing their own policies and procedures pertaining to fixed assets. In addition, DBHDS has not allocated or prioritized the appropriate resources to ensure that such internal policies and procedures over fixed assets are present.

Recommendation

Management should create, 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 agency systems or other processes.

Why the APA Audits Access Management for the Medicaid Management Information System

The Medicaid Management Information System stores protected health information for nearly one million individuals and it is used to process approximately \$8 billion in medical claims annually. While the Medicaid Management Information System is operated by a contractor, the Department of Medical Assistance Services (Medical Assistance Services) is the system owner and they are responsible for ensuring that the Medicaid Management Information System is managed in accordance with the Commonwealth's Information Security Standard (Security Standard). To evaluate Medical Assistance Services' management of access for the Medicaid Management Information System, we compared internal practices to those required by the Security Standard, which resulted in the following three findings with recommendations.

Improve Access Reviews of the Medicaid Management Information System – Repeat

Condition

Medical Assistance Services has not updated the Interagency Agreement with the Department of Social Services (Social Services) to require Social Services to perform an annual review of their Medicaid Management Information System users. Additionally, Medical Assistance Services' annual review of the Medicaid Management Information Systems' users continue to only include employees who are newly hired, separated, or transferred. Their review of access does not include current Medical Assistance Services employees who have not changed positions.

Criteria

The Commonwealth's Information Security Standard, SEC 501-08 (Security Standard), Section 8.1 AC-2(j), requires that agencies review user accounts and privileges annually.

Consequence

The Medicaid Management Information System is used to update Medicaid eligibility information and it is used to process Medicaid claims that total approximately \$8 billion annually. Without reviewing user accounts and privileges annually, Medical Assistance Services and Social Services cannot confirm that user access is current and reasonable based on the user's job responsibilities. This increases the risk of unauthorized users being able to access and make changes to protected health and financial information within the system.

Cause

Medical Assistance Services' Policy Division has not updated the Interagency Agreement to include a requirement for Social Services to review Medicaid Management Information System access. Additionally, Medical Assistance Services has not expanded their annual review of Medicaid Management Information Systems users because they are still in the process of evaluating software that will allow them to automate the process.

Recommendation

Even though access to the Medicaid Management Information System is suspended for inactive users, we recommend that Medical Assistance Services' Policy Division update the Interagency Agreement with Social Services to include an annual review of their Medicaid Management Information System users. Additionally, Medical Assistance Services should include all of their Medicaid Management Information System users in their annual review of access. Together, both of these actions will enable Medical Assistance Services, the system owner, ensure that user accounts and privileges are current and reasonable for the Medicaid Management Information System.

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

Condition

Medical Assistance Services does not have documentation that facilitates system owners and supervisors in evaluating and approving privileges in the Medicaid Management Information System. As a result of the lack of documentation, supervisors are instructing the Information Security Officer (ISO) on the privileges each employee should have; however, supervisors are not provided a detailed description of the screens and transactions the employee will be able to view and change. Supervisors need this information to facilitate an appropriate evaluation of the employee's system access. Additionally, system owners have not documented the combinations of privileges that create an internal control weakness. Without system owners documenting which privileges create a weakness, the Information Security Officer cannot question the appropriateness of the privileges a supervisor approves for an employee.

Criteria

The Commonwealth's Information Security Standard, SEC 501-08 (Security Standard), 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.

The Medical Assistance Services User Acknowledgement and Responsibilities Agreement for the Medicaid Management Information System requires that the authorizing (requesting) supervisor only request privileges that the employee needs to perform their job duties and tasks.

Consequence

Two of the eleven employees tested, 18 percent, had privileges within the Medicaid Management Information System application that they did not need to perform their job duties. The authorizing and granting of this access by the supervisor and the ISO, respectively, violates the principle of least privileges and creates an internal control weakness within the application that could result in fraud or errors.

Cause

According to management, they did not have the resources and staff to devote time to document and define all the privileges that are controlled through access clusters in the Medicaid

Management Information System. However, management has since hired a Documentation Specialist to document the privileges within the Medicaid Management Information System.

Recommendation

In addition to continuing to document the privileges in the Medicaid Management Information System, management should:

- Require system owners to document privilege combinations that create an internal control weakness, which could be done by developing a conflict matrix.
- Require system owners to provide supervisors and the Information Security Officer documentation that facilitates them in evaluating current access and future requests.
- Require system owners to train supervisors on the different privileges they are allowed to request.

Identify a Back-up for Medicaid Management Information System Administration and Document the Process

Condition

The Information Security Officer (ISO) is the only individual at Medical Assistance Services who can create, modify, or delete access clusters in the Medicaid Management Information System. Additionally, there is no documentation of how the ISO executes these tasks.

Criteria

The Commonwealth's Information Security Standard, SEC 501-08 (Security Standard), AC-2-COV (h), requires at least two individuals have administrative accounts to provide continuity of operations. Security Standard AC-2-COV requires agencies to document management practices for administering accounts.

Consequence

Without a back-up or documentation on how to administer access, Medical Assistance Services risks not being able to manage access to the Medicaid Management Information System.

Cause

According to management, the complexities of the Medicaid Management Information System and limited staffing has caused Medical Assistance Services to not identify a back-up or document how the ISO creates, modifies, or deletes access clusters.

Recommendation

We recommend that management identify a back-up for administering access to the Medicaid Management Information System. Additionally, we recommend that management document the process for administering Medicaid Management Information System access.

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 contained sensitive protected health 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 Commonwealth's Information Security Standard and the 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 contracts these security compliance reviews to an outside auditor. We reviewed the 2013 security compliance audit report issued by Internal Audit and echo their findings and recommendations below, some of which are repeats from prior audits.

Correct Operating Environment and Security Issues Identified by their Security Compliance Audit

Condition

Medical Assistance Services' Internal Audit Division (Internal Audit) review dated January 31, 2014, evaluated Medical Assistance Services operating environment and security business processes for the period July 1, 2012, through June 30, 2013. The review found that Medical Assistance Services had generally implemented adequate processes for compliance with the Commonwealth's Information Security Standard, SEC 501-7.1 (Security Standard), and the Health Insurance Portability and Accountability Act (HIPAA) Security Rule; however, there were 15 noted exceptions involving the following controls:

- Contingency Planning
- Configuration Management
- Mobile Device Management
- Physical Security Procedures
- Risk Assessment Procedures
- Audit Logging and Monitoring
- Password Configuration Management
- Logical Access Controls
- Personal Information Protection
- Contract Management
- Sensitive Documentation Handling Procedures
- Training Materials
- Email Disclaimer Requirements
- Publicly Accessible Content Reviews
- Policies and Procedures Reviews

Criteria

The Security Standard requires 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

Medical Assistance Services has increased the 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

Medical Assistance Services has not adequately applied the appropriate resources and staff to address the information technology security needs of the agency and address exceptions reported in the Internal Audit Division's prior review.

Recommendation

We recommend that Medical Assistance Services continue to follow its corrective action plans for the 15 identified weaknesses. Medical Assistance Services should also, develop or acquire the necessary resources to ensure that appropriate controls are applied over its sensitive information systems and data.

Why the APA Audits Financial System Application Access

Medical Assistance Services utilizes an internal financial system that is the agency's system of record for financial activity. Financial information in the agency's internal system impacts the financial information reported in the Commonwealth Accounting and Reporting System (CARS). The Commonwealth Accounting and Reporting System is the financial system that the Department of Accounts uses to report the Commonwealth's financial activity. Because both the internal financial system and CARS are critical to financial reporting to the Commonwealth, management at Medical Assistance Services must properly manage access to ensure the integrity of the data within these systems. To evaluate Medical Assistance Services' management of access for its financial system and CARS, we compared internal practices to those required by the Commonwealth's Information Security Standard, which resulted in the following two findings, one for each system, with recommendations.

Strengthen Financial System Application Access

Condition

Medical Assistance Services is using the default roles and responsibilities instead of configuring the system based on the needs of the system users. In addition, Medical Assistance Services is not consistently reviewing audit records; and not documenting access roles and responsibilities in a way that allows managers to evaluate if their employees have the correct level of access, nor has it documented conflicting modules or responsibilities that could be used to override separation of duties controls.

Criteria

The Commonwealth's Information Security Standard, SEC 501-08 (Security Standard):

1. Section 8.5. CM-7 requires organizations to configure the information system to provide only the essential capabilities required for the business function of the information system;
2. Section 8.3 AU-6 requires organizations to review and analyze information system audit records at least every thirty days for indications of inappropriate or unusual activity; and
3. Section 8.1 AC-2(b) and (c) requires that access privileges be specified and conditions for group membership be established.

Consequence

Because Medical Assistance Services did not modify the default roles and responsibilities, the fiscal services administrator responsible for user account management had roles and responsibilities that were not required for his job responsibilities. Furthermore, because there is no understanding of the default roles and responsibilities and no documentation of the access roles

and responsibilities, incorrect access was assigned and was subsequently approved by management during the annual review of access.

In addition, Inconsistent reviews of audit records by Medical Assistance Services may result in inappropriate or unusual activity going undetected by management. Finally, without documenting conflicting modules and roles and providing that documentation to the managers requesting and reviewing access, Medical Assistance Services risks granting access that could create a separation of duties issue. Because the system interfaces directly with the Commonwealth Accounting and Reporting Systems, the Commonwealth's official financial record, weak internal controls could question the integrity of the Commonwealth's financial records.

Cause

Medical Assistance Services elected to use the default settings established by the vendor and did not reconfigure the system based on their needs. Furthermore, the system administrators did not know how to reconfigure the fiscal services administrator's role.

Additionally, Medical Assistance Services has not implemented a policy to review the audit records according to the Security Standard requirement, nor is there a policy to document the access roles and responsibilities or the conflicting modules or responsibilities. Finally, management has been using their general knowledge of the roles as they have been requesting and reviewing access.

Recommendation

We recommend that Medical Assistance Services' management gain an understanding of the roles and responsibilities for all default settings and adhere to the Security Standard and reconfigure default setting based on the user's needs. Furthermore, we recommend that Medical Assistance Services, implement a process to review audit records every thirty days and have an individual independent from the System Administrator review the audit records. Finally, Medical Assistance Services should document the access roles and responsibilities and conflicts in a way that will allow managers to adequately evaluate if access is reasonable and provides proper separation of duties surrounding fiscal transactions.

Confirm that Application Access is Appropriate

Condition

Medical Assistance Services did not remove access to the Commonwealth Accounting and Reporting System (CARS) and the 1099 Adjustment and Reporting Systems (ARS) for individuals who no longer needed access. One individual retained CARS access for 64 business days after termination, while ten individuals retained access to either CARS or ARS when it was no longer needed for their job responsibilities. We were unable to determine how long these individuals retained access when it was not needed.

Criteria

The Commonwealth's Information Security Standard, SEC 501-08 (Security Standard), AC-6 and AC-2-COV, states that access should be granted based on the principle of least privilege and be promptly removed when no longer required. Furthermore, the CAPP Manual states that the each agency's CARS Security Officer (CSO) is responsible for a comprehensive system of internal controls over CARS tables and files.

Consequence

Allowing users to retain access to CARS and ARS when it is no longer needed increases the risk of unauthorized transactions in these systems.

Cause

The CSO did not confirm with supervisors whether individuals still required CARS and ARS access. Furthermore, the CSO did not confirm that the Department of Accounts deleted access for the terminated employee.

Recommendation

The CSO's semi-annual review process should include verifying, with the individual's supervisor, whether CARS and ARS access is still needed. In addition, the CSO should implement a process to confirm that access is deleted based on the request made to the Department of Accounts.

Why the APA Audits Managed Care Organization Capitation Rates

Managed care organizations provide access to health benefits and care for the majority of Medicaid beneficiaries in the Commonwealth. In fiscal year 2014, seven managed care organizations received capitation payments totaling more than \$2 billion. Capitation rates are determined by an actuary and approved by Medical Assistance Services. Medical Assistance Services and each managed care organization sign a contract containing the agreed upon rates. We compare the signed contracts to the capitation rates used by the system to calculate the capitation payments and found discrepancies.

Rates Used by the System Should be Supported by a Signed Contract with the Same Rates

Condition

Medical Assistance Services did not have the correct capitation rates in three Managed Care Organization (MCO) contracts. While the rates used by the system to calculate payments agreed to the actuary's rates and MCOs were paid the correct rates, the contracts signed by management and the MCOs did not contain the same rates. There were 80 inconsistent capitation rates for one MCO contract for the period of July 1, 2013, through December 31, 2013. In addition, there was another inconsistent capitation rate for two MCO signed contracts during the contract amendment period of January 1, 2014, through June 30, 2014.

Criteria

The Commonwealth of Virginia Department of General Services Agency Procurement and Surplus Property Manual requires that all goods or services be billed by the contractor at the contract price.

Consequence

Using capitation rates in the system that do not agree to the signed contract increases the risk of MCOs getting paid rates that have not been actuarially determined, negotiated, and approved by the Commonwealth. While this could result in overpayments or underpayments by the Commonwealth, we did not note any.

Cause

The Provider Reimbursement Division and the Health Care Services Division did not include the correct capitation rates in some of the contracts signed by the Medical Assistance Services Director and the Managed Care Organizations.

Recommendation

Management at Medical Assistance Services should review contract capitation rates included in the contract for accuracy prior to signing.

Why the APA Audits IT Systems Backup and Restoration Policies and Procedures

The Department of Social Services (Social Services) collects, manages, and stores significant volumes of personal and financial data within its mission critical systems. The ability to access this information or restore this information is critical to ensure that essential social service programs can be administered as intended in the event of a systems failure. To evaluate information technology systems backup and restoration policies and procedures, we compared Social Services' policies and procedures to those required by the Commonwealth's Information Security Standard, which resulted in the following finding.

Document IT Systems Backup and Restoration Policy and Procedure

Condition

Social Services does not have documented internal procedures that outline the actions needed to validate backup integrity and ensure efficient and effective mission-critical data restoration.

Criteria

While Social Services can demonstrate that they monitor the Information Technology (IT) Partnership's infrastructure backup and restoration efforts, the Commonwealth's Information Security Standard, SEC 501-08 (Security Standard), Section CP-9, requires that an agency develop documented backup restoration plans to support restoration of its applications. Agency applications do not fall under the IT Partnership's purview.

Consequence

Adopting a formalized policy and procedure will increase the ability for Social Services to consistently govern application backup and restoration efforts and ensure that clear and documented expectations exist between the agency and the IT Partnership. A formalized policy and procedure will also reduce the risk of Social Services' inability to successfully restore mission essential functions that are dependent on software applications that are hosted on the IT Partnership's servers.

Cause

Social Services did not have a formal documented process due to a misunderstanding of the distinction between an IT Disaster Recovery Plan and an IT Backup and Restoration Policy. While some aspects of both governing documents are similar, the Security Standard maintains that they are separate and distinct documents that serve different purposes.

Recommendation

Social Services should dedicate the necessary resources to create a policy and procedure that document the established IT systems backup and restoration process.

Why the APA Audits Access in the Financial Accounting Analysis System

Social Services uses the Financial Accounting Analysis System as its official system of record for financial activity related to social services programs administered by Social Services, including the Temporary Assistance for Needy Families program and the Supplemental Nutrition Assistance Program, among other programs. Because of the critical nature of this financial system, Social Services' management must ensure that all necessary precautions are taken to ensure the integrity of the data within its system. To determine if adequate database security, including system access, was maintained, we compared the practices of Social Services to those required by the Commonwealth's Information Security Standard, which resulted in the following finding.

Monitor Actions of Employees Granted Temporary Access in FAAS

Condition

Social Services does not have a mechanism in place to actively monitor transactions of employees in the Accounts Payable Division that are temporarily granted additional access within the Financial Accounting Analysis System (FAAS). Temporary access is not included as part of an employee's normal job duties, and can cause a conflict with the structure of internal controls normally maintained within the Accounts Payable Division.

Criteria

The Commonwealth's Information Security Standard, SEC 501-08 (Security Standard), Section 8.1, AC2-Account Management, part f., states that agencies should specifically authorize and monitor the use of guest or anonymous and temporary accounts.

Consequence

Without effective monitoring of users with temporary access, Social Services cannot provide assurance that transactions processed, during the period which temporary privileges were granted, are properly authorized or not entered and approved by the same employee. For example, an employee that is normally authorized to create vendors within FAAS may be able to also initiate payments to vendors they create during a period of temporary access.

Cause

Temporary access is generally given when there is a staffing shortage for a short period of time and invoices must be keyed or approved within a certain time frame to maintain reasonable business flow. Social Services has established some controls over this access, as temporary access is end-dated in the system, and a paper file of any unusual or temporary requests is maintained to ensure that the temporary access is immediately removed when the access is no longer needed.

Recommendation

The Accounts Payable Division should coordinate with the financial systems team to ensure that temporary access is monitored appropriately and adequate compensating controls are in place during the periods when temporary access is necessary. The creation of some type of mechanism to monitor the use of temporary access will allow Social Services to further ensure that no unauthorized or inappropriate transactions occurred as a result of the granting of temporary access.

Why the APA Audits Data Required by the Federal Funding Accountability and Transparency Act

Social Services receives federal funds and disburses some of the funds to local departments of social services and other contractors as necessary to administer social services programs within the Commonwealth. The Federal Funding Accountability and Transparency Act requires that entities receiving federal funds report quarterly if those funds beyond a certain threshold are disbursed to other entities. This reporting mechanism provides transparency of these financial transactions for citizens by allowing them to see on a federal website how these tax dollars are being spent. To confirm that Social Services submitted the information required by the Federal Funding Accountability and Transparency Act, we reviewed the data made publicly available on the federal website serving as the repository of this data, which resulted in the following finding.

Ensure Compliance with the Federal Funding Accountability and Transparency Act

Condition

Social Services did not complete its fourth quarter financial reporting required by the Federal Funding Accountability and Transparency Act (FFATA). Based on a review of information reported on the FFATA Subaward Reporting System (FSRS), we were not able to locate any reporting done for the June 30, 2014, quarter for Foster Care, the Child Care Development Fund, or the Social Services Block Grant.

Criteria

FFATA and 2 CFR §170 require Social Services to report information to the federal government for awards of certain federal funds that Social Services makes to subrecipients.

Consequence

Failure to comply with FFATA and corresponding regulations prevents the federal government and taxpayers from knowing which entities are receiving federal funds through Social Services.

Cause

Due to turnover within the Federal Grants Reporting unit within the Division of Finance during July 2014, the June 30, 2014, quarterly FFATA reporting was not completed as required.

Recommendation

Social Services should ensure that all required reporting is completed within the established timeframes as required by FFATA.

Why the APA Audits Access to Mission Critical Systems

Social Services collects, manages, and stores significant volumes of personal and financial data within its mission critical systems. Monitoring access to the mission critical systems to ensure that only authorized users are accessing the systems in accordance with necessary job functions is essential to ensure that social service programs can be administered as intended and proper payments are provided to eligible recipients. To evaluate access to the mission critical systems, we compared Social Services’ review of systems access to those required by the Commonwealth’s Information Security Standard, which resulted in the following finding.

Review User Accounts and Privileges for Mission Critical Systems – Repeat

Condition

Management at Social Services is not annually reviewing user accounts and privileges for reasonableness as required. We found that management did not conduct an annual review of access for two of its mission critical systems.

Criteria

The Commonwealth’s Information Security Standard, SEC 501-07.1 (Security Standard), Section 8.1.AC-2(j), requires that agencies review user accounts and privileges annually.

Consequence

Social Services uses Automated Program to Enforce Child Support (APECS) to manage the Child Support Enforcement Program and the Energy Assistance System (EAS) to manage the Low Income Household Energy Assistance Program. Without reviewing user accounts and privileges annually, Social Services’ management cannot make the assertion that user access is current and reasonable based on the user’s job responsibilities. In effect, this increases Social Services’ risk of unauthorized transactions taking place within these systems.

Cause

Social Services has not performed annual access reviews for several of its mission critical systems because it lacks a process that communicates user access privilege listings and review responsibilities. Management is in the process of developing an automated process to facilitate their reviews, which is taking longer to implement than the estimated completion date of July 31, 2014, that was provided during the prior year audit.

Recommendation

Social Services should develop a mechanism to supply system owners and managers with a listing of user accounts and their privileges. Social Services should also develop a plan to ensure an annual review of all mission critical systems. By meeting this requirement of the Security Standard, Social Services will be able to ensure that user accounts and privileges are current and reasonable.

Why the APA Audits Access to the Application Benefit Delivery Automation Project System

Social Services uses the Application Benefit Delivery Automation Project (ADAPT) system to administer the Supplemental Nutrition Assistance Program, the Temporary Assistance for Needy Families program, and the Medicaid program. Ensuring the appropriate internal controls system within the Application Benefit Delivery Automation Project system is essential to ensure that these social service programs were administered as intended and proper payments were provided to eligible recipients. To evaluate Social Services’ internal controls surrounding ADAPT, we compared management’s related controls to those required by the Commonwealth’s Information Security Standard, which resulted in the following finding.

Develop Workable Solutions to Maintain Appropriate Balance of Internal Controls – Repeat

Condition

The Information Security Officer (ISO) at Social Services is not maintaining the appropriate detective controls to determine what users with elevated levels of access are doing within the Application Benefit Delivery Automation Project (ADAPT) system.

Criteria

The Commonwealth’s Information Security Standard, SEC 501-07.1 (Security Standard), Section 2.5.4, requires that the ISO implement and maintain the appropriate balance of preventative, detective, and corrective controls for agency information systems commensurate with data sensitivity, risk, and systems criticality.

Consequence

ADAPT is the case management system for the Supplemental Nutrition Assistance Program (SNAP), Temporary Assistance for Needy Families (TANF), and Medicaid programs. Without the ISO maintaining the appropriate detective controls to determine what users with elevated levels of access are doing within ADAPT, management cannot assure itself that unauthorized transactions did not take place.

Cause

During the prior year audit, we found that the Secretary of Health and Human Resources tasked the Department of Medical Assistance Services (Medical Assistance Services) to perform a project to determine if discrepancies in information critical to eligibility determination existed between the Commonwealth’s different case management systems. While performing this project, Medical Assistance Services identified several discrepancies between the systems. As a result, Social Services then tasked several employees to update information in ADAPT.

When granting access to ADAPT, management elected to give these individuals access allowing them to make updates within the application. The access granted allowed these employees to override the eligibility determination rules, and make updates directly to the supporting database.

While the ISO originally objected to providing these individuals with this level of access, the access was later granted without any compensating controls.

The ISO has a mechanism to track the actions of database administrators, which have capabilities similar to the employees in question within ADAPT. The ISO had the ability to track what these users were doing in ADAPT. However, the Divisions within Social Services which authorize the users' elevated levels of access have not worked with the ISO to confirm that enough information has been provided in order to implement detective controls. Therefore, the ISO is unable to review what tasks these users are performing because the listing of cases authorized to be updated have not been provided to the Division of Information Technology. The ISO continues to not be able to develop an expectation as to what would be considered a reasonable modification.

Recommendation

Going forward, the Divisions within Social Services which authorize users to have elevated levels of access should work with the ISO to confirm that enough information has been provided in order to implement detective controls. By doing such, the ISO will be able to assure the Commissioner that Social Services' systems are properly secured and that information has not been incorrectly altered.

Why the APA Audits Change Management Processes for Sensitive Applications

Social Services is currently in the process of implementing a new system that the Commonwealth will use to manage multiple aspects of its larger programs, including Medicaid eligibility determination. The implementation of new applications and systems is sometimes necessary to ensure that the Commonwealth is operating in its most effective and efficient capacity, and also can be necessary to ensure that policy changes for program administration are incorporated as intended. When these types of changes occur, it is critical to ensure that all necessary components of program administration are instituted as required, and systems security measures are sufficiently applied. To determine if appropriate change management policies and procedures are present, we compared the practices of the Social Services to those required by the Commonwealth’s Information Security Standard, which resulted in the following finding.

Implement and Monitor a Change Management Process for Sensitive Applications – Repeat

Condition

While Social Services has approved a formal change management policy and process since our last audit, Social Services has not yet implemented or monitored this process in its information technology (IT) environment. Social Services continues to work towards implementing its change management process for sensitive applications.

Criteria

The Commonwealth's Information Security Standard, SEC 501-08 (Security Standard), Section CM-1 and CM-3-COV, requires agencies to implement its formal change control policy and procedures.

Consequence

Not implementing the new change management policy and procedures may introduce inconsistent and improper changes to the Social Services IT environment, which may result in unreliable, unavailable, or compromised sensitive data.

Cause

Social Services originally indicated in its corrective action plan that it would “establish, implement and monitor a policy for ‘Change Management Process’ ... [by] September 30, 2014.” However, since Social Services only approved its change management policy in September 2014, implementing and monitoring this policy has not yet been possible.

Recommendation

Social Services should continue to follow their corrective action plan by dedicating the necessary resources to implement and monitor the recently approved change management policy and process over its IT environment.



Martha S. Mavredes, CPA
Auditor of Public Accounts

Commonwealth of Virginia

Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

December 12, 2014

The Honorable Terence R. McAuliffe
Governor of Virginia

The Honorable John C. Watkins
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, 2014. 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 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, 2014, 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, 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

The Agencies of the Secretary of Health and Human Resources' management has responsibility for establishing and maintaining internal control and complying with applicable laws and regulations. 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 five agencies.

Comprehensive Services for At-Risk Youth and Families

Administrative controls at the Department of Education, reported under a separate report
Revenues and expenses
Subrecipient monitoring

Department of Behavioral Health and Developmental Services

Accounts receivables
Capital outlay
Fixed asset management
Budgeting
Operational expenses
Payroll expenses
Contract procurement and management
Institutional revenues
Community Service Board contracts
Information system security
Systems access controls

Department of Health

Accounts Receivable
Federal revenues, expenses, and compliance for:
 Special Supplemental Nutrition Program for Women, Infants, and Children
 Child and Adult Care Feeding Program

Payroll expenses
Support for local rescue squads
Collection of fees for services
Cooperative agreements between Health and local government, which includes:
 Aid to local governments
 Allocation of costs
 Reimbursement from local governments

Accounts Payable
Information system security
System access controls

Department of Medical Assistance Services

Federal revenues, expenses, and compliance for:
Medicaid program
Money Follows the Person Program

Accounts receivable
Accounts payable
Contract management
System access controls
Utilization units

Department of Social Services

Federal revenues, expenses, and compliance for:
Child Care and Development Fund Cluster
Social Services Block Grant
Child Support Enforcement
Foster Care Title IV-E

Eligibility for:
Temporary Assistance for Needy Families
Low Income Household Energy

Budgeting and cost allocation
Network and System Security
Child Support Enforcement Asset Accuracy
Supplemental Nutrition Assistance Program Supplemental Information
Accounts Payable

The following agencies under the control of the Secretary of Health and Human Resources are not material to the Comprehensive Annual Financial Report for the Commonwealth of Virginia nor have a federal program that is required to be audited as part of the Statewide Single Audit. 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
Virginia Board for People with Disabilities
Virginia Foundation for Healthy Youth

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, 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.

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, 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. The Agencies record their financial transactions in the Commonwealth Accounting and Reporting System 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.

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 within the body of this report, we identified certain deficiencies in internal control over financial reporting that we consider to be material weaknesses and other deficiencies that we consider to be significant deficiencies in internal control.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial information will not be prevented, or detected and corrected on a timely basis. We consider the deficiencies entitled "Improve Access Controls for the Crossroads System," "Account for All WIC EBT Food Instruments and Investigate Errors," "Record Accurate Time and Effort Reporting," "Complete Local Agency Monitoring Reviews," "Submit Invoices for WIC Rebates and Medicaid Claims," and "Improve Controls over Federal Reporting WIC", which are described within the body of this report to constitute a material weakness. As such, they will be reported as a material weakness in the Independent Auditor's Report on Internal Control over Financial Reporting and on Compliance and Other Matters Based on an Audit of the Financial Statements Performed in Accordance with Government Auditing Standards, included in the Commonwealth of Virginia Single Audit Report for the year ended 2014.

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, described within the body of this report, to be significant deficiencies.

We also found that, except for the possible effects of the matter described in the Material Noncompliance paragraph below, the Agencies of the Secretary of Health and Human Resources, as defined in the Audit Scope and Methodology section above, complied, in all material respects, with the types of compliance requirements tested for the Statewide Single Audit that could have a direct and material effect on each major program tested.

The Agencies have taken adequate corrective action with respect to audit findings reported in the prior year that are not repeated in this report.

Lack of Evidence Supporting Compliance

As described within the body of this report, we were unable to obtain sufficient appropriate audit evidence supporting the compliance of the Department of Health's with 10.557 Special Supplemental Nutrition Program for Women, Infants, and Children (WIC) Program as described in findings entitled "Improve Access Controls for the Crossroads System," "Account for All WIC EBT Food Instruments and Investigate Errors," "Record Accurate Time and Effort Reporting," "Complete Local Agency Monitoring Reviews," "Submit Invoices for WIC Rebates and Medicaid Claims," and "Improve Controls over Federal Reporting WIC"; consequently we were unable to determine whether the Department of Health complied with those requirements applicable to that program.

As such, we will issue a qualified opinion on the Special Supplemental Nutrition Program for Women, Infants, and Children Program in the Independent Auditor's Report on Compliance for Each Major Federal Program; Report on Internal Control Over Compliance; and Report on Schedule of Expenditures of Federal Awards Required by OMB Circular A-133 for the Commonwealth of Virginia.

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/alh



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 26, 2015

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, 2014. We concur with the findings except as noted in our detailed responses, and a copy of our corrective action plan has been provided under a separate cover memo.

Over the past few years, VDH has been challenged by the USDA to manage several feeding programs. Development, enhancement, and integration of these feeding programs with existing business processes has been a multiyear effort, while continuing to address many other public health needs across the Commonwealth.

VDH's implementation of Crossroads, a new WIC information management and Electronic Benefits Transfer (EBT) system, is one of the primary challenges faced by the agency over the past few years. Virginia was the first state to simultaneously implement a new information management system and EBT system, which was necessary to replace an obsolete legacy system and meet a federal mandate to operate an EBT system. VDH, under the guidance of its federal grantor, successfully transitioned hundreds of retailers across the Commonwealth to the EBT process with no service interruptions to the hundreds of thousands of Virginia residents that benefit from this critically important program. As we continue implementing our corrective action plan, we will share these issues and recommendations with other VDH programs as well as state and federal partners to improve the overall success of our public health programs.

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 Levine, MD, MPH
State Health Commissioner





COMMONWEALTH of VIRGINIA

DEBRA FERGUSON, Ph.D.
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: Debra Ferguson, Ph.D.
SUBJECT: *Response to Management Comments – FY 2014 APA Audit*
DATE: January 21, 2015

The following are the Department of Behavioral Health and Developmental Services (DBHDS) responses to the management comments from the APA's FY 2014 audit of the Department.

Improve Database Security:

The Department concurs with the audit comment and continues to work towards implementing secure practices.

The expected date of implementation for this response is 9/1/2015, and the responsible party is Marcie Stout – DBHDS Chief Information Security Officer.

Improve IDOLS Security:

The Department concurs with the audit comment and will continue to enhance security over all systems. As a part of this effort, the Department will seek funding from the Governor for the 2016-2018 biennium.

The responsible party for this response is Marcie Stout – DBHDS Chief Information Security Officer.

Develop and Submit an Information Technology Audit Plan:

DBHDS has had an inventory of sensitive IT systems since June of 2012. In addition, the required IT audit plan was submitted to VITA on December 15, 2014.

In order to complete the audit plan, DBHDS submitted a budget request to the Governor for funds to be allocated to hire an Information Security Auditor. This request was rejected. Any

internal redeployment of dollars to fund a position would take away limited resources necessary to fund mission critical services for individuals served by the department.

Improve Controls Over Systems Access:

The Department concurs with this finding. A notification process was put in place at DBHDS in FY 2014 to cover access controls at Central Office. This notification process, along with an automated access deletion process, is currently being put in place at all of the DBHDS facilities. The Department takes seriously the need to have strong systems controls, and this issue is being addressed. To help ensure the successful implementation of this response, systems access will continue to be monitored by the DBHDS Office of Internal Audit and the DBHDS Information Security Officer.

The expected date of implementation for this response is June 30, 2015, and the responsible parties are Randy Sherrod – DBHDS Internal Audit Director and Marcie Stidham-Stout – DBHDS Chief Information Security Officer.

Improve Controls over Hours Worked by Wage Employees:

In the two exceptions noted, we concur that oversights were made; however in each instance, the controls in place allowed for the discovery that the hours worked exceeded 1,508 hours during the measurement period of May 1, 2013 – April 30, 2014.

The Department will continue to monitor the hours worked by wage employees at Central Office and all facilities. The responsible party for this response is Randy Sherrod – DBHDS Internal Audit Director.

Improve Controls over the VNAV System:

The Department concurs with this finding. Notice will be given to all DBHDS facilities to remind them that contribution snapshot reconciliations are to be done timely, that all facilities should have policies and procedures related to VNAV, and that access to the system include proper segregation of duties. In addition, VRS will be offering training on VNAV in spring 2015; which will help DBHDS with implementation of this response and internal processes related to this system.

Implementation of this will be completed by June 30, 2015 and will be monitored by the DBHDS Office of Internal Audit. The responsible party for this response is Randy Sherrod – DBHDS Internal Audit Director.

Improve Controls over Payroll:

The Department concurs with this finding. The DBHDS Office of Internal Audit issued the findings and accepted the respective responses from the facilities where testwork was completed. Follow-up reviews will be done in Fiscal Year 2016 to ensure compliance with the responses given.

Implementation of this response should be completed by June 30, 2015. The responsible party for this response is Randy Sherrod – DBHDS Internal Audit Director.

Improve Controls over Physical Inventory:

The Department concurs with this finding. DBHDS will continue to make every effort to adhere to CAPP Manual Topic 30505 - Physical Inventory. The three facilities that were cited for non-compliance regarding timeliness of fixed asset inventories will have a full fixed asset inventory completed by June 30, 2015.

Central Office has no remaining fixed assets as the assets cited by the APA have been removed from FAACS. DBHDS Central Office will ensure that fixed asset transactions are recorded timely in the future.

Implementation of this response will be monitored by the DBHDS Office of Internal Audit. The responsible party for this response is Phil Peter – DBHDS Fiscal and Grants Director.

Create Policies and Procedures for Fixed Assets:

The Department concurs with this finding. DBHDS will ensure that all facilities have policies and procedures related to fixed assets in addition to those published in the CAPP Manual.

Implementation of this response will be monitored by the DBHDS Office of Internal Audit and will be completed by June 30, 2015. The responsible party for this response is Phil Peter – DBHDS Fiscal and Grants Director.



COMMONWEALTH of VIRGINIA
Department of Medical Assistance Services

CYNTHIA B. JONES
DIRECTOR

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

January 21, 2015

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

Dear Ms. Mavredes:

We have reviewed your Draft Report Findings on the Audit of the Agencies of the Secretary of Health and Human Resources for the Fiscal Year Ending June 30, 2014. We concur with your findings assigned to DMAS and will continue corrective action as indicated below.

Finding 1 - Improve Access Reviews of the Medicaid Management Information System - Repeat

Condition

Medical Assistance Services has not updated the Interagency Agreement with the Department of Social Services (Social Services) to require Social Services to perform an annual review of their Medicaid Management Information System users. Additionally, Medical Assistance Services' annual review of the Medicaid Management Information Systems' users continue to only include employees who are newly hired, separated, or transferred. Their review of access does not include current Medical Assistance Services employees who have not changed positions.

Recommendation

Even though access to the Medicaid Management Information System is suspended for inactive users, we recommend that Medical Assistance Services' Policy Division update the Interagency Agreement with Social Services to include an annual review of their Medicaid Management Information System users. Additionally, Medical Assistance Services should include all of their Medicaid Management Information System users in their annual review of access. Together, both of these actions will enable Medical

Assistance Services, the system owner, ensure that user accounts and privileges are current and reasonable for the Medicaid Management Information System.

Corrective Action Plan:

As part of its agreement process, DMAS will update/modify the Interagency Agreement with the Department of Social Services to reflect the Medicaid Management Information System (MMIS) annual user review. The Policy and Research Division has developed proposed modification language to the Interagency Agreement. The Policy Division expects the Interagency Agreement to be modified by March 31, 2015.

Additionally, DMAS will conduct an annual review for its MMIS users.

DMAS will develop some type of automated process to provide system owners and/or employee managers a user listing with assigned privileges for annual review, and document resulting annual reviews for its MMIS system.

This effort is dependent upon the purchase and implementation of an automated tool such as a workflow product to assist in providing tools for System Owner and Data Owner reviews to occur more routinely on a documented basis.

Information Management (IM) Division is exploring other options at this time, to determine if existing DMAS-owned COTS products may satisfy this review requirement. Even if this is so, there is still a development period that must occur.

Controls Implemented

DMAS suspends MMIS user accounts as soon as notified, or when a 30 day period of inactivity occurs, automated account suspension occurs. Deletions occur in a timely basis.

DMAS suspends other user accounts for DMAS systems upon notification. Deletions occur in a timely basis.

Responsible Persons:

- Mukundan Srinivasan, DMAS Information Management Division Director;
- Brian McCormick, Policy and Research Division Director
- Theresa Fleming, DMAS Information Security Officer, Office of Compliance and Security, Information Management Division

Estimated Implementation Date: December 31, 2015

Finding 2 - Create Formal Documentation that Facilitates Controlling Privileges in the Medicaid Management Information System

Condition

Medical Assistance Services does not have documentation that facilitates system owners and supervisors in evaluating and approving privileges in the Medicaid Management Information System. As a result of the lack of documentation, supervisors are instructing the Information Security Officer (ISO) on the privileges each employee should have; however, supervisors are not provided a detailed description of the screens and transactions the employee will be able to view and change. Supervisors need this information to facilitate an appropriate evaluation of the employee's system access. Additionally, system owners have not documented the combinations of privileges that create an internal control weakness. Without system owners documenting which privileges create a weakness, the Information Security Officer cannot question the appropriateness of the privileges a supervisor approves for an employee.

Recommendation

In addition to continuing to document the privileges in the Medicaid Management Information System, management should:

- Require system owners to document privilege combinations that create an internal control weakness, which could be done by developing a conflict matrix.
- Require system owners to provide supervisors and the Information Security Officer documentation that facilitates them in evaluating current access and future requests.
- Require system owners to train supervisors on the different privileges they are allowed to request.

Corrective Action Plan:

DMAS will conduct an annual review for its MMIS users which will include user listing and transaction assignment listing for review.

DMAS will develop some type of automated process to provide system owners and/or employee managers a user listing with assigned privileges for annual review, and document resulting annual reviews for its MMIS system.

This effort is dependent upon the purchase and implementation of an automated tool such as a workflow product to assist in providing tools for System Owner and Data Owner reviews to occur more routinely on a documented basis.

Information Management (IM) Division is exploring other options at this time, to determine if existing DMAS-owned COTS products may satisfy this review requirement. Even if this is so, there is still a development period that must occur.

Responsible Persons:

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

Estimated Implementation Date: December 31, 2015

Finding 3 – Identify a Back-up for Medicaid Management Information System Administration and Document the Process

Condition

The Information Security Officer (ISO) is the only individual at Medical Assistance Services who can create, modify, or delete access clusters in the Medicaid Management Information System. Additionally, there is no documentation of how the ISO executes these tasks.

Recommendation

We recommend that management identify a back-up for administering access to the Medicaid Management Information System. Additionally, we recommend that management document the process for administering Medicaid Management Information System access.

Corrective Action Plan:

DMAS has designated a backup ISO for administering MMIS access and will be training the backup to perform the following functions:

1. Change a cluster (add/delete)
2. Add a new cluster
3. Remove a cluster

A new APEX application to manage the MMIS access clusters has been developed. The input to the application is authorized by the user's management. Currently, the application is in User Acceptance Testing (UAT) and not yet in production.

Responsible Persons:

- Mukundan Srinivasan, DMAS Information Management Division Director;

- Theresa Fleming, DMAS Information Security Officer, Office of Compliance and Security, Information Management Division

Estimated Implementation Date: December 31, 2015

Finding 4 – Correct Operating Environment and Security Issues Identified by their Security Compliance Audit

Condition

Medical Assistance Services' Internal Audit Division (Internal Audit) review dated January 31, 2014, evaluated Medical Assistance Services operating environment and security business processes for the period July 1, 2012 through June 30, 2013. The review found that Medical Assistance Services had generally implemented adequate processes for compliance with the VITA Information Security Standard (SEC 501-7.1) and the Health Insurance Portability and Accountability Act (HIPAA) Security Rule; however, there were 15 noted exceptions involving the following controls:

- Contingency Planning
- Configuration Management
- Mobile Device Management
- Physical Security Procedures
- Risk Assessment Procedures
- Audit Logging and Monitoring
- Password Configuration Management
- Logical Access Controls
- Personal Information Protection
- Contract Management
- Sensitive Documentation Handling Procedures
- Training Materials
- Email Disclaimer Requirements
- Publicly Accessible Content Reviews
- Policies and Procedures Reviews

Recommendation

We recommend that Medical Assistance Services continue to follow its corrective action plans for the 15 identified weaknesses. Medical Assistance Services should also, develop or acquire the necessary resources to ensure that appropriate controls are applied over its sensitive information systems and data.

Corrective Action Plan:

The Information Management Division, the Office of Compliance and Security, the Human Resources Division, and the Fiscal and Purchases Division have been working together to address the findings of the DMAS Security Compliance Audit dated

January, 31, 2014. To date, nine of the 15 findings have been resolved. Listed is a summary of the corrective action plan for each finding.

1. Contingency plans were not approved, distributed, or updated.

The Information Management Division and the Office of Compliance and Security completed a second redraft of the DMAS HIPAA Contingency and Disaster Recovery Plan on December 18, 2014.

2. Change management approvals were not documented (Financial System).

The Information Management Division implemented a configuration control process for the Financial System applications on April 27, 2014.

3. Controls for mobile devices should be established and implemented.

The Information Management Division, the Office of Compliance and Security, and the Human Resources Division finalized the Mobile Device (BYOD) Policy effective October 15, 2014. The Policy was signed by Agency Head, and announced to Agency October 30, 2014.

4. Physical access controls should be strengthened.

DMAS has upgraded its badge access system to Kastle and is in the process of updating its processes and procedures. Additional reports are also being considered. The Office of Compliance and Security is coordinating with the Human Resources Division (HR). The estimated completion date is May 1, 2015.

5. DMAS risk management processes, including data sensitivity classification and system inventory procedures, need improvement.

DMAS Office of Compliance and Security (OCS) prepared a Statement of Work (SOW) to obtain a formal Risk Assessment (RA) at DMAS on its Agency applications. The SOW was posted, bids were reviewed, and a vendor selection was made. The Information Management Division expects the RA to begin in January 2015 with an estimated completion date of June 30, 2015.

6. Audit logging and monitoring procedures should be implemented.

The Information Management Division addressed the fiscal services administrator's role by designing a new role called DMAS_FISCAL_ADMIN and provides the minimum access needed to provision user accounts. We have revoked the financial services administrator's access to the SYSADMIN role. The Information Management Division developed a process to provide the

SYSADMIN use log and auto-provide to the ISO and the ISO has verified this is working.

A new application has been created to review the application access logs and the SYSADMIN logs are now sent to the DBA Manager and the ISO (Security Help email id) on a monthly basis. The corrective actions were completed on December 1, 2014.

7. Strong passwords are not enforced for DMAS information systems (Financial System).

The Information Management Division completed corrective action on December 1, 2014. The password reset process (for user password lockout) has been modified so that, passwords are not automatically unlocked, unless the user contacts the DBA directly for assistance.

8. Procedures for requesting, authorizing, documenting, and reviewing access to DMAS information systems should be strengthened.

The DMAS Office of Compliance and Security (OCS) has pursued a workflow product to assist in providing tools for System Owner and Data Owner reviews to occur more routinely on a documented basis. This is pending funding to allow for purchase. Due to purchase/implementation delay, the estimated completion date is May 1, 2015.

9. Social security numbers are not redacted or masked.

The DMAS Information Management Division is working on updating the application involved to remove the outdated field (containing the social security number) to a generic sequence number. The Financial System has been updated to use a generic sequence number for the Vendor number field. Corrective action was tested and completed on December 13, 2014.

10. DMAS does not have an updated contract with the agency service provider.

The Information Management (IM) Division worked closely with VITA to establish/modify its MOU to include SLAs as required. Weekly meetings occur with VITA/NG. IAG-404 was signed by the Agency Head on February 10, 2014.

11. Shred bins located throughout the DMAS facility remain unlocked.

All shred bins were locked on May 13, 2014. A DMAS agency-wide announcement was made on that date.

12. DMAS training materials should be enhanced.

The Office of Compliance and Security (OCS) is in the process of updating its training materials to more clearly include the concept of separation of duties and intellectual property rights. This corrective action was delayed due to other higher-priority work; the estimated completion date is May 1, 2015.

13. DMAS email disclaimer was not enforced.

The Agency-wide email disclaimer for use with all outgoing email messaging was reviewed and approved by the DMAS Security Advisory Committee (SAC). The email disclaimer was implemented on September 2, 2014. An agency-wide announcement was made on that same date.

14. Procedures to review publicly accessible content should be improved.

The Information Management (IM) Division is pursuing a change control process for its web content. An application to handle the change control workflow for the web content is in development. The system is patterned after an existing configuration management system for development. Documentation of the process has been drafted. The application is currently in User Acceptance Testing (UAT). The expected completion date is February 15, 2015.

15. DMAS policies and procedures were not updated.

DMAS Office of Compliance and Security (OCS) has updated its Policy and Standards. Procedures were delayed due to VITA transformation activities, and limited staff availability. DMAS plans to address these issues but the effort has been delayed due to other higher priority work. The estimated completion date is May 1, 2015.

Responsible Persons:

- Mukundan Srinivasan, DMAS Information Management Division Director
- Theresa Fleming, DMAS Information Security Officer, Office of Compliance and Security, Information Management Division
- Kathleen Guinan, DMAS Human Resources Division Director
- Karen Stephenson, DMAS Fiscal and Purchases Division Director

Estimated Implementation Date:

Finding	Date Completed	Estimated Completion Date
1. Contingency plans were not approved, distributed, or updated.	12/18/2014	-
2. Change management approvals were not	04/27/2014	-

documented (Financial System).		
3. Controls for mobile devices should be established and implemented.	10/30/2014	-
4. Physical access controls should be strengthened.	-	05/01/2015
5. DMAS risk management processes, including data sensitivity classification and system inventory procedures, need improvement.	-	06/30/2015
6. Audit logging and monitoring procedures should be implemented.	12/01/2014	-
7. Strong passwords are not enforced for DMAS information systems (Financial System).	12/01/2014	-
8. Procedures for requesting, authorizing, documenting, and reviewing access to DMAS information systems should be strengthened.	-	05/01/2015
9. Social security numbers are not redacted or masked.	12/13/2014	-
10. DMAS does not have an updated contract with the agency service provider.	02/10/2014	-
11. Shred bins located throughout the DMAS facility remain unlocked.	05/13/2014	-
12. DMAS training materials should be enhanced.	-	05/01/2015
13. DMAS email disclaimer was not enforced.	09/02/2014	-
14. Procedures to review publicly accessible content should be improved.	-	02/15/2015
15. DMAS policies and procedures were not updated.	-	05/01/2015

Finding 5 – Strengthen Financial System Applications Access

Condition

Medical Assistance Services is using the default roles and responsibilities instead of configuring the system based on the needs of the system users. In addition, Medical Assistance Services is not consistently reviewing audit records; and not documenting access roles and responsibilities in a way that allows managers to evaluate if their employees have the correct level of access, nor has it documented conflicting modules or responsibilities that could be used to override separation of duties controls.

Recommendation

We recommend that Medical Assistance Services' management gain an understanding of the roles and responsibilities for all default settings and adhere to the Commonwealth's Security Standard and reconfigure default setting based on the user's needs. Furthermore, we recommend that Medical Assistance Services, implement a process to review audit records every thirty days and have an individual independent from the System Administrator review the audit records. Finally, Medical Assistance Services should document the access roles and responsibilities and conflicts in a way that will allow managers to adequately evaluate if access is reasonable and provides proper separation of duties surrounding fiscal transactions.

Corrective Action Plan:

1. The Fiscal Division will examine existing staffing roles and needs of our division and the agency, re-evaluate the respective responsibilities assigned in the Financial System Application and redefine those requiring more restrictions to functions and/or menus in the Financial Systems applications modules currently in use.

We addressed the fiscal services administrator's role by designing a new role called DMAS_FISCAL_ADMIN, which provides the minimum access needed to provision user accounts. We have revoked the financial services administrator's access to the SYSADMIN role.

2. A new application has been created to review the application access logs and the SYSADMIN logs are now sent to the DBA Manager and the ISO (Security Help email id) on a monthly basis.
3. The Fiscal Division will document the capabilities of each responsibility in use and any potential conflicts with other modules and/or responsibilities.

Responsible Persons:

- Mukundan Srinivasan, DMAS Information Management Division Director;
- Karen Stephenson, DMAS Fiscal Division Director
- Theresa Fleming, DMAS Information Security Officer, Office of Compliance and Security, Information Management Division

Estimated Implementation Date: June 30, 2015

Finding 6 – Confirm that Application Access is Appropriate

Condition

Medical Assistance Services did not remove access to the Commonwealth Accounting and Reporting System (CARS) and the 1099 Adjustment and Reporting Systems (ARS) for individuals who no longer needed access. One individual retained CARS access for

64 business days after termination, while ten individuals retained access to either CARS or ARS when it was no longer needed for their job responsibilities. We were unable to determine how long these individuals retained access when it was not needed.

Recommendation

The CSO's semi-annual review process should include verifying, with the individual's supervisor, whether CARS and ARS access is still needed. In addition, the CSO should implement a process to confirm that access is deleted based on the request made to the Department of Accounts.

Corrective Action Plan:

The Fiscal Division will establish a new semiannual review process to assess CARS and ARS accesses.

On a semiannual basis beginning SFY 2015, the Fiscal Systems Administrator (CSO) will provide respective Managers with a list of their staff and the corresponding CARS and/or ARS accesses. Managers will be required to review and certify that the access is still appropriate based on the current role and responsibilities of the employee. All employees with access to CARS and/or ARS will be included in this review and certification process.

Responsible Persons:

- Mukundan Srinivasan, DMAS Information Management Division Director;
- Karen Stephenson, DMAS Fiscal Division Director
- Theresa Fleming, DMAS Information Security Officer, Office of Compliance and Security, Information Management Division

Estimated Implementation Date: May 31, 2015

Finding 7 - Rates Used by the System Should be Supported by a Signed Contract with the Same Rates

Condition

Medical Assistance Services did not have the correct capitation rates in three Managed Care Organization (MCO) contracts. While the rates used by the system to calculate payments agreed to the actuary's rates, the contracts signed by management and the MCOs did not contain the same rates. There were 80 inconsistent capitation rates for one MCO contract for the period of July 1, 2013 through December 31, 2013. In addition, there was another inconsistent capitation rate for two MCO signed contracts during the contract amendment period of January 1, 2014 through June 30, 2014.

Recommendation

Management at Medical Assistance Services should review contract capitation rates included in the contract for accuracy prior to signing.

Corrective Action Plan:

DMAS has confirmed that the rates paid were the correct rates. The discrepancy between the correct rates and the rates in the contract totaled \$418, an error rate of 0.00002%. DMAS has prepared contract amendments for the three plans with incorrect rates in the contract. These contract amendments should be completed by the end of January 2015.

Controls Implemented

Before submitting the contracts signed by the plans to the DMAS Director for her signature, DMAS will add an additional control requiring the Provider Reimbursement division to compare the final rates to the rates in the contracts.

Responsible Persons:

- Bill Lessard, DMAS Provider Reimbursement Division Director;
- Bryan Tomlinson, DMAS Health Care Service Division Director

Estimated Implementation Date: January 31, 2015

If you have any questions, please do not hesitate to contact our Director of Internal Audit, Paul Kirtz.

Sincerely,



Cynthia B. Jones



COMMONWEALTH of VIRGINIA
DEPARTMENT OF SOCIAL SERVICES
Office of the Commissioner

Margaret Ross Schultze
COMMISSIONER

January 28, 2015

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

Dear Ms. Mavredes:

Attached please find the Virginia Department of Social Services Response and Plan of Correction to the 2014 review of the Department by the Auditor of Public Accounts.

We concur with the audit findings and look forward to working with you on implementation of this plan.

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, or at (804) 726-7384.

Sincerely,

A handwritten signature in black ink, appearing to read "Margaret Ross Schultze".

Margaret Ross Schultze

AGENCY OFFICIALS



Department of Medical Assistance Services

Cynthia B. Jones– Director



Department of Social Services

Margaret R. Schultze– Commissioner



Department of Behavioral Health and Developmental Services

Debra Ferguson, Ph.D. – Commissioner



Department of Health

Marissa Levine, MD, MPH – Commissioner



Office of Comprehensive Services for At-Risk Youth and Families

Susan C. Clare – Executive Director