STATE OF FLORIDA AUDITOR GENERAL

Operational Audit

Report No. 2016-027
October 2015

DEPARTMENT OF VETERANS' AFFAIRS

Sherrill F. Norman, CPA
Auditor General

Executive Director of the Department of Veterans' Affairs

Section 20.37, Florida Statutes, creates the Department of Veterans' Affairs. The head of the Department is the Governor and Cabinet. The Executive Director of the Department is appointed by the Governor with the approval of the three members of the Cabinet and is subject to confirmation by the Senate. Mike Prendergast served as Executive Director during the period of our audit.

The team leader was Joanna Slater and the audit was supervised by Matthew Tracy, CPA. For the information technology portion of this audit, Art Wahl, CPA, was the team leader.

Please address inquiries regarding this report to Matthew Tracy, CPA, Deputy Auditor General, by e-mail at matthewtracy@aud.state.fl.us or by telephone at (850) 412-2749.

This report and other reports prepared by the Auditor General are available at:

www.myflorida.com/audgen

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 • 111 West Madison Street • Tallahassee, FL 32399-1450 • (850) 412-2722

DEPARTMENT OF VETERANS' AFFAIRS

SUMMARY

This operational audit of the Department of Veterans' Affairs focused on resident care assessments and collections, Residents' Deposits Trust Fund accounts, and selected information technology (IT) controls. The audit also included a follow-up on the findings noted in our report No. 2014-007. Our audit disclosed the following:

Resident Care Assessments and Collections

Finding 1: As similarly noted in prior audit reports, most recently in our report No. 2014-007, Department controls were not always sufficient to effectively safeguard moneys collected.

Finding 2: Annual financial information used to verify resident income and determine resident assessments was not always timely updated at the Domiciliary.

Residents' Deposits Trust Fund Accounts

Finding 3: The Sims and Nininger Nursing Homes did not always effectively implement Department policies and procedures for the administration of Residents' Deposits Trust Fund accounts.

Finding 4: As similarly noted in our report No. 2014-007, some nursing homes did not always effectively implement Department policies and procedures to ensure that resident account balances complied with Medicaid asset limit requirements.

Finding 5: Some resident account funds at the Nininger Nursing Home were not timely disbursed upon the discharge or death of the resident.

Selected Information Technology Controls

Finding 6: The Department had not established a risk management program and categorized IT risks in accordance with governing rules. In addition, Department monitoring of IT controls need improvement.

Finding 7: The Department's Continuity of Operations Plan and certain backup and recovery policies and procedures need enhancement.

Finding 8: The Department had not timely obtained and reviewed the independent service auditor's report related to the controls designed and established by the Department's vendor for MatrixCare, an electronic health record system used by the Department to process administrative, billing, financial, and clinical record transactions. In addition, the Department had not established a policy and procedure for monitoring third-party IT service provider compliance with Department requirements.

Finding 9: Department IT policies and procedures need improvement.

Finding 10: The Department did not always timely deactivate IT user access privileges upon an employee's separation from Department employment. Additionally, the Department did not always ensure that network access privileges were necessary.

BACKGROUND

The Department of Veterans' Affairs (Department) is a Cabinet agency created to assist all former, present, and future members of the Armed Forces of the United States and their dependents in preparing claims for and securing compensation, hospitalization, career training, and other benefits or privileges to which such persons are, or may become, entitled to under Federal or State law or regulation as a result of their service in the Armed Forces.[1] The Department provides advocacy and representation for many of the State's more than 1.5 million veterans and their families.[2]

Pursuant to State law,[3] the Department provides long-term residential health care and domiciliary services for honorably discharged veterans through six nursing homes and a Domiciliary (assisted living facility). State law[4] requires the Department to operate the nursing homes under the State provisions for licensed health care facilities. Table 1 provides a listing of, and information related to, Department-operated residential facilities.

Table 1
Veterans' Nursing Homes and Domiciliary
Number of Available Beds, Residents, Authorized Staff Positions, and Total Resident Care Assessments, Resident Care Collections, and Residents' Deposits Trust Fund Balances

		As of June 30, 2014			2013-14 Fiscal Year		At June 30, 2014
Facility	**Location**	**Number of Available Beds**	**Number of Residents**	**Number of Authorized Staff Positions**	**Total Resident Care Assessments**	**Total Resident Care Collections**	**Total Residents' Deposits Trust Fund Balances**
Emory L. Bennett State Veterans' Nursing Home (Bennett Nursing Home)	Daytona Beach	120	117	137	$12,696,003	$12,488,969	$65,359
Douglas T. Jacobson State Veterans' Nursing Home (Jacobson Nursing Home)	Port Charlotte	120	120	139	12,576,537	12,534,481	25,770
Baldomero Lopez State Veterans' Nursing Home (Lopez Nursing Home)	Land O'Lakes	120	119	144	13,705,856	12,486,654	7,373
Alexander Nininger State Veterans' Nursing Home (Nininger Nursing Home)	Pembroke Pines	120	118	141	12,809,973	12,218,503	66,692
Clifford C. Sims State Veterans' Home (Sims Nursing Home)	Panama City	120	120	141	12,127,256	11,289,987	104,953
Clyde E. Lassen State Veterans' Nursing Home (Lassen Nursing Home)	St. Augustine	120	120	157	13,483,684	12,602,847	20,017
Robert H. Jenkins Jr. State Veterans' Domiciliary Home (Domiciliary)	Lake City	150	144	67	3,801,933	3,784,309	61,523
Totals		**870**	**858**	**926**	**$81,201,242**	**$77,405,750**	**$351,687**

Source: Department records.

[1] Section 292.05(1), Florida Statutes.
[2] Department 2013-2014 *Annual Report,* dated November 11, 2014.
[3] Chapter 296, Florida Statutes.
[4] Sections 296.33(4) and 400.23, Florida Statutes.

On March 19, 2014, the Department contracted with a vendor for MatrixCare, an electronic health record system used by the Department to process administrative, billing, financial, and other clinical record transactions. In June 2014, the Department began pilot implementation of MatrixCare and, as of August 2014, any transactions not part of a previous claim were processed in MatrixCare. Prior to the implementation of MatrixCare, the Department utilized the UltraCare for Windows database (UltraCare) to manage the financial and clinical functions of the Department's nursing homes and Domiciliary. As necessary, the Department updates existing UltraCare records, and MatrixCare, to reflect modifications to existing benefits and claims.

FINDINGS AND RECOMMENDATIONS

RESIDENT CARE ASSESSMENTS AND COLLECTIONS

The operating costs of the nursing homes and Domiciliary have been historically funded through the Grants and Donations Trust Fund, Operations and Maintenance Trust Fund, and the State Homes for Veterans' Trust Fund. State law[5] requires nursing home and Domiciliary residents to contribute to the cost of their care based upon their level of income. In addition to resident contributions, each nursing home and the Domiciliary receives per diem payments, based on the facility's occupancy, from the United States Department of Veterans' Affairs and, for eligible residents, payments from third-parties such as private insurance and the Medicare and Medicaid programs.

Finding 1: Collection Safeguards

Appropriate safeguards for moneys collected are essential for the prevention or detection of theft or loss. Such safeguards include restrictively endorsing collections immediately upon receipt, documenting transfers of collections between employees, and reconciling accounting system records to initial collection receipts or logs. During the 2013-14 fiscal year, the nursing homes and Domiciliary collected revenues totaling approximately $77 million. As part of our audit, we evaluated Department policies and procedures and the collection controls at the nursing homes and Domiciliary and noted:

- *Restrictive endorsement of collections*. Department policies and procedures did not specify the employee position responsible for endorsing checks received at the nursing homes and Domiciliary that were not addressed to a resident. In addition, at the Lopez, Nininger, and Sims Nursing Homes, non-resident checks were not restrictively endorsed at the point and time of receipt.
- *Transfer of custodial responsibility*. Bennett, Lopez, and Nininger Nursing Home staff did not document the transfer of collections from one employee to another. In response to our audit inquiry, Department management indicated that, subsequent to the period of our audit, the Lopez Nursing Home established a chain of custody form for collections. In addition, Department management acknowledged in response to our audit inquiry that Department policies and

[5] Sections 296.10 and 296.37, Florida Statutes, require that the total amount of the residents' contributions be to the fullest extent possible, but in no case exceed the actual cost of operating and maintaining the home.

procedures did not provide for an appropriate Departmentwide document to track the transfer of funds from one employee to another.

- *Records reconciliation.* Nininger Nursing Home staff did not reconcile pre-numbered collection receipts to the Cash Receipt Register used to prepare bank deposits.

We noted similar issues in prior audit reports, most recently in our report No. 2014-007, finding No. 1. Effective collection controls provide greater assurance that funds will be appropriately safeguarded and accounted for and that any theft or loss, should it occur, will be timely detected.

Recommendation: We again recommend that Department management enhance collection policies and procedures to provide for appropriate collection controls at the nursing homes and Domiciliary. Such policies and procedures should specify the employee position responsible for endorsing checks and address controls designed to ensure that checks are restrictively endorsed at the time of receipt, all transfers of collections between employees are documented, and collection receipts are timely reconciled to bank deposit records.

Finding 2: Annual Financial Update

Department policies and procedures required that every January 1st, nursing home and Domiciliary business office staff update each resident's financial status utilizing information provided on a Financial Data Update form to determine if there were any changes in the amounts or types of moneys received by the resident. The policies and procedures specified that a form was to be completed by each resident, their family members, or legal guardian, as appropriate, and returned along with supporting documentation (e.g., monetary award letters and bank statements) to the facility's business office no later than February 15th each calendar year.

As part of our audit, we evaluated nursing home and Domiciliary controls for ensuring that residents contributed to the cost of their care based upon their level of income. Our audit tests disclosed that, for the annual resident income determinations tested at the six nursing homes, the determinations were properly documented. However, our testing at the Domiciliary disclosed that annual resident financial updates were not always timely completed. Specifically, our examination of the Domiciliary's Annual Financial Update Tracking log disclosed that as of May 5, 2015, 15 of 134 residents had not returned a completed Financial Data Update form and 64 residents had returned completed forms from 1 to 68 days (an average of 22 days) after the February 15th deadline.

As part of our audit, we noted that Domiciliary management had taken steps to obtain the overdue forms. However, as the Financial Data Update form provides resident financial information necessary for accurately determining resident assessments, the facility's timely receipt of forms is critical.

Recommendation: We recommend that Domiciliary management continue to take appropriate steps to promote the timely receipt of Financial Data Update forms and all supporting documentation in accordance with Department policies and procedures.

RESIDENTS' DEPOSITS TRUST FUND ACCOUNTS

Pursuant to State law,[6] the Department administers Residents' Deposits Trust Funds in separate local bank accounts for each of the nursing homes and the Domiciliary. State law requires that, within each Trust Fund, accounts be maintained for each resident without charge and provides that the residents may voluntarily withdrawal all personal moneys deposited and interest earned.

Finding 3: Residents' Deposits Trust Fund Policies and Procedures

In our report No. 2014-007, finding No. 3, we noted that some nursing homes and the Domiciliary did not effectively implement Department policies and procedures for the administration of Residents' Deposits Trust Fund accounts. To better ensure that resident moneys were not subject to unauthorized disbursement, among other things, Department policies and procedures[7] required that a bank signature card be on file at the bank and updated as needed by nursing home and Domiciliary staff to reflect authorized check signers. The policies and procedures also specified that the individuals permitted to sign Residents' Deposits Trust Fund account checks included each facility's Administrator, Director of Nursing, Social Services Director, Risk Manager, and Minimum Data Set Coordinator.

As part of our audit, we performed audit tests at the six nursing homes and the Domiciliary and noted that, generally, the nursing homes and Domiciliary had effectively implemented Department Residents' Deposits Trust Fund policies and procedures. However, we also found that the Sims Nursing Home's bank account signature authorizations were not always timely removed upon employment termination or did not appear necessary. Specifically, we found that the Sims Nursing Home Administrator who resigned on September 16, 2013, was not removed as an authorized check signer on one account until February 25, 2015. Additionally, we noted that the Deputy Executive Director of the Department was listed as an authorized signer for one bank account, which did not appear to be necessary and in accordance with Department policies and procedures.

Finally, we noted that Sims and Nininger Nursing Home staff did not always document authorizations of disbursements from resident accounts as required by Department policies and procedures. Specifically:

- Our test of ten Sims Nursing Home resident check disbursement transactions made during the period January 2014 through February 2015 disclosed that for four checks totaling $3,230, Sims Nursing Home staff did not obtain written authorizations for the disbursements. Although Nursing Home documentation indicated that verbal authorizations had been obtained for the disbursements, the signatures of two witnesses to support each verbal authorization had not been obtained as required by Department policies and procedures.
- Our test of ten Nininger Nursing Home resident check disbursement transactions made during the period January 2014 through February 2015 disclosed that for a $3,600 spousal support check, Nininger Nursing Home staff did not obtain written authorization for the disbursement, nor the signatures of two witnesses to support the resident's verbal authorization for the disbursement.

Although the Department had established policies and procedures for the administration of Residents' Deposits Trust Fund accounts, Sims and Nininger Nursing Home staff did not always effectively

[6] Sections 296.12 and 296.38, Florida Statutes.

[7] Department *Business Office Procedures*, Section I-4, dated November 1, 2011.

implement or adhere to the requirements. Consequently, the risk that resident moneys will be subjected to unauthorized disbursement is increased.

Recommendation: We recommend that Sims and Nininger Nursing Home management take steps to ensure that Nursing Home staff implement and adhere to established Department policies and procedures for the administration of Residents' Deposits Trust Fund accounts.

Finding 4: Medicaid Asset Limit

Residents in Department facilities may receive assistance from the Medicaid program to pay for services received. Federal regulations[8] provide that nursing home facilities must notify each resident who receives Medicaid benefits when the amount in the resident's account reaches the Supplemental Security Income (SSI) resource limit (specified as the Medicaid asset limit) for one person ($2,000). Federal regulations specify that if the amount in a resident's account, in addition to the resident's other nonexempt resources, reaches the SSI resource limit, the resident may become ineligible for Medicaid or SSI.

Pursuant to Federal regulations, Department policies and procedures[9] required that when a Medicaid-participating resident's trust fund (RTF) account balance was near or at $1,500, nursing home staff were to discuss with the resident or resident's representative a spending plan and the potential for Medicaid ineligibility. Further, Department policies and procedures required that when a Medicaid-participating RTF account balance reached $1,800, the resident or resident's representative was to be notified in writing that the resident was approaching the Medicaid asset limit of $2,000 and that if the resident's balance exceeded $2,000, Medicaid benefits may be discontinued. Department policies and procedures also specified that if a Medicaid-participating RTF account balance exceeded the $2,000 limit, the Medicaid program was to be notified.

In our report No. 2014-007, finding No. 5, we noted that the Department had not implemented effective policies and procedures to ensure that resident account balances complied with Medicaid asset limit requirements. As part of our audit, we examined selected Medicaid-participating RTF account balances at the Department's six nursing homes to determine whether, as applicable, nursing home staff adhered to Department policies and procedures for the Medicaid asset limit.[10] Our audit procedures disclosed that:

- Bennett Nursing Home staff could not provide documentation demonstrating that, for nine of ten RTF account balances selected, a spending plan and the potential for becoming ineligible for Medicaid, had been discussed with the applicable resident (or their representative) when the RTF account balances were near or at $1,500. For seven of the nine accounts, Bennett Nursing Home staff could also not provide documentation demonstrating that the Department sent a letter notifying the applicable resident or their representative that the Medicaid asset limit was being approached when the RTF account balances reached $1,800. For another account, although Bennett Nursing Home staff documented spending plan discussions with the applicable resident, no documentation was available demonstrating that the Department sent a letter notifying the resident or their representative that the Medicaid asset limit was being approached when the RTF account balance reached $1,800.

[8] Title 42, Section 483.10(c)(5), Code of Federal Regulations.

[9] Department Standards and Procedures, *Resident Trust Fund Medicaid Asset Limit – Section – III – 2*, dated April 5, 2013.

[10] The Domiciliary did not bill for Medicaid services during the period January 2014 through February 2015.

- For two RTF account balances selected at the Sims Nursing Home, staff could not provide documentation demonstrating that a spending plan and the potential for becoming ineligible for Medicaid had been discussed with the applicable resident (or their representative) when the RTF account balances were near or at $1,500. In addition, for these two accounts, Sims Nursing Home staff could not provide documentation demonstrating that the Department sent a letter notifying the applicable resident or their representative that the Medicaid asset limit was being approached when the RTF account balances reached $1,800.

As part of our audit, we also noted that, while Department management had taken steps to establish effective Medicaid asset limit policies and procedures, the policies and procedures did not specify the anticipated costs that could be factored into, or the resources that could be excluded from, the determination of an RTF account balance for Medicaid asset limit purposes. Absent adherence to Department policies and procedures that clearly specify Medicaid asset limit requirements, the risk is increased that residents may not be timely and properly notified when the amounts in their RTF accounts approach the Medicaid asset limit.

Recommendation: We again recommend that Department management ensure that Medicaid-participating residents are timely and properly notified of potential Medicaid program ineligibility in accordance with Department policies and procedures. We also recommend that Department management further enhance policies and procedures to specify the anticipated costs that may be factored into, and the resources that may be excluded from, the determination of an RTF account balance for Medicaid asset limit purposes.

Finding 5: Resident Account Close-Out Process

State law[11] requires that, upon the death of a resident with personal funds deposited with a facility, the facility must convey to the resident's designated representative within 30 days, the resident's funds, including interest, and a final accounting of those funds. Pursuant to State law, Department policies and procedures specified that designated staff were to complete an audit on all accounts of discharged or deceased residents and that resident funds were to be disbursed to the resident or their beneficiary within 30 days. For the period January 2014 through February 2015, Department management identified a total of 435 resident accounts at the nursing homes and Domiciliary that required close-out due to the discharge or death of the resident.

As part of our audit, we examined documentation for 104 resident accounts (15 at each of the six nursing homes and 14 at the Domiciliary) that required close-out due to the discharge or death of the resident during the period January 2014 through February 2015 and noted that, for five of the six nursing homes and the Domiciliary, resident accounts were properly reviewed and funds were timely disbursed. However, our audit procedures found that for 2 of the 15 accounts examined at the Nininger Nursing Home, staff disbursed resident funds, totaling $50 and $108, 35 and 49 days, respectively, after the former resident's discharge or death. In response to our audit inquiry, Nininger Nursing Home staff indicated that in one instance, the resident's liabilities had to be paid prior to closing the account and disbursing the funds.

[11] Section 400.022(1)(h)(4), Florida Statutes.

To ensure accountability and compliance with State law, timely close-out of a resident's account upon the resident's death or discharge is essential.

Recommendation: We recommend that Nininger Nursing Home management take steps to ensure that all resident funds are timely disbursed to the resident or their beneficiary in accordance with State law.

SELECTED INFORMATION TECHNOLOGY CONTROLS

An entitywide information technology (IT) control program is the foundation of an IT control structure and a reflection of senior management's commitment to addressing control risks. An effective IT control program establishes, among other things, a risk management program, appropriate continuity of operations and disaster recovery plans, effective controls for monitoring the activities of third-party IT service providers, comprehensive and current IT policies and procedures, and IT access controls.

Finding 6: Risk Management Program

Agency for Enterprise Information Technology (AEIT) rules[12] specify that State agencies are to implement a documented risk management program, including risk analysis for high-impact information resources. Those rules also specify that State agencies are to categorize IT resource risks according to Federal Information Processing Standards (FIPS) Publication 199. In addition, effective monitoring involves testing IT controls to determine whether the controls are appropriately designed and operating effectively to achieve management's control objectives.

As part of our audit, we noted that the Department completed a risk assessment survey[13] on March 4, 2015. The survey responses detailed the status of the Department's information security program and identified areas where the Department's program needed improvement. Specifically, the Department identified that it had not:

- Categorized IT resource risks in accordance with FIPS Publication 199.
- Implemented a risk management program.

In addition, our audit procedures disclosed certain security monitoring controls that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility compromising Department data and IT resources. However, we have notified appropriate Department management of the specific issues.

A documented, approved, and implemented risk management program helps management effectively manage risks to IT resources and data and ensures the appropriate testing of critical IT controls. The absence of such a risk management program may have also contributed to the issues identified in Findings 7 through 9.

[12] AEIT Rule 71A-1.020, Florida Administrative Code. Effective July 1, 2014, Chapter 2014-221, Laws of Florida, created the Agency for State Technology (AST) within the Department of Management Services and authorized a type two transfer of all records; property; administrative authority; and administrative rules in Chapters 71A-1 and 71A-2, Florida Administrative Code, of the AEIT to the AST.

[13] The *Florida Enterprise Information Security Risk Assessment Survey* was conducted by the AST.

Recommendation: We recommend that Department management implement a documented and approved risk management program and categorize IT risks in accordance with FIPS Publication 199. In addition, we recommend that Department management take steps to monitor and test the effectiveness of all critical IT controls identified by the risk management program when implemented.

Finding 7: Continuity of Operations and Disaster Recovery

AEIT rules[14] specify that IT resources identified as critical to the continuity of governmental operations are to have documented disaster recovery plans to provide for the continuation of critical State agency functions in the event of a disaster. Those rules require that disaster recovery plans be tested at least annually and the results of the annual exercise be documented and note the plan procedures that were successful and any necessary plan modifications.

AEIT rules also specify that data and software essential to the continued operation of critical State agency functions are to be mirrored to an off-site location or backed up regularly with a current copy stored at an off-site location. Off-site locations are effective when geographically removed from the original site so that the data and software are protected from the same disaster events.

As part of our audit, we examined the Department's policies, procedures, and plans for continuity of operations, including disaster recovery, as well as for backup and recovery of critical IT resources and data. Our examination disclosed that, while the Department had developed a Continuity of Operations Plan (COOP)[15] that included a disaster recovery plan for the Department's IT resources, enhancements were needed in Department COOP and disaster recovery procedures. Specifically, we found that:

- The COOP was dated July 2012 and had not been formally approved by Department management. Additionally, the COOP had not been updated to incorporate MatrixCare.
- While the Department had established a draft disaster recovery procedure for UltraCare, the procedure had not been finalized and indicated that the proposed process needed to be tested and evaluated for insertion into the COOP.
- The Department had established an off-site location for regularly backing up critical data. However, the off-site location was less than 50 miles from the primary computing facility, reducing its effectiveness as it was not geographically separated from a disaster affecting the primary computing facility.
- UltraCare data was periodically backed up at the off-site location. However, the Department had not established a documented or approved policy for UltraCare data backup.
- The Department indicated in response to our audit inquiry that it had conducted a test of its plan to recover UltraCare data in December 2014. However, this test was not conducted at the off-site location and the results of this test had not been documented.

Although the Department is transitioning the management of financial and clinical functions from UltraCare to MatrixCare, in response to our audit inquiry, Department management indicated that, due to Medicare billing requirements, the Department is to keep UltraCare fully available until August 1, 2018, and, until 2023, provide read-only access to UltraCare data.

[14] AEIT Rule 71A-1.012(4), Florida Administrative Code.

[15] A COOP is a documented plan detailing how an agency will respond to incidents that could jeopardize the organization's core mission.

The establishment of a current, management-approved COOP, including a disaster recovery plan, as well as policies and procedures for backing up and recovering critical IT systems and data provides greater assurance that critical Department operations will continue in the event of a disaster. In addition, establishment of a geographically separate off-site location for regularly backing up critical Department data will reduce the risk posed from a disaster.

Recommendation: We recommend that Department management approve an updated COOP that includes enhanced back-up location provisions, establish policies and procedures for backing up and recovering all critical IT systems and data, and document recovery test results.

Finding 8: Evaluation of Service Auditor's Reports

As noted in the ***BACKGROUND***, on March 19, 2014, the Department contracted with a vendor for MatrixCare, an electronic health record system used by the Department to process administrative, billing, financial, and clinical record transactions. The contract included provisions requiring compliance with, among other things, minimum service levels, background checks, and security awareness training. In June 2014, the Department began pilot implementation of MatrixCare and, as of August 2014, any transactions not part of a previous claim were performed in MatrixCare. As a result of the critical functionality provided by MatrixCare, Department management must rely on the controls established by the vendor to ensure the accuracy and completeness of MatrixCare information.

However, our audit procedures disclosed that, although service auditor's reports[16] on the effectiveness of the controls established by the vendor for MatrixCare and related information were available, the Department, prior to our audit inquiry in March 2015, had not requested or reviewed such reports.[17] In addition, we noted that the Department had not established a policy and procedure for monitoring third-party IT service provider compliance with Department requirements.

Absent the timely request, receipt, and review of a service auditor's report, the Department has limited assurance that the MatrixCare information relied upon for administrative, billing, financial, and clinical record transactions is accurate and complete. Additionally, the establishment of a policy and procedure for monitoring the activities of third-party IT service providers would provide Department management greater assurance that such providers are complying with Department requirements.

Recommendation: We recommend that Department management timely request, obtain, and document review of service auditor's reports on the effectiveness of vendor controls established for MatrixCare. Additionally, to better ensure compliance with Department requirements, we recommend that Department management establish a policy and procedure for monitoring the activities of third-party IT service providers.

[16] A service auditor's report, as described by the American Institute of Certified Public Accountants, Statement on Standards for Attestation Engagement No. 16, *Reporting on Controls at a Service Organization*, provides information and auditor conclusions related to a service organization's controls. Service organizations make service auditor's reports available to user organizations to provide assurances related to the effectiveness of the service organization's relevant internal controls.

[17] The most-recent service auditor's report for MatrixCare and related information was dated October 22, 2014.

Finding 9: IT Policies and Procedures

Each IT function needs complete, current, and well-documented policies and procedures to describe the scope of the function and its activities. Sound policies and procedures, with documented management approval, provide benchmarks against which compliance can be measured and contribute to an effective control environment by addressing identified risks.

As noted in Finding 6, the Department completed a risk assessment survey and identified areas where the Department's information security program needed improvement. In addition to identifying the need for policies and procedures as discussed in Findings 7 and 8, the survey also identified that the Department had not:

- Kept selected Department security documentation up-to-date;
- Documented data security policies and procedures;
- Created a system security plan;
- Documented secure coding policies;
- Documented device configuration standards; and,
- Documented network security procedures for perimeter control and secure wireless implementation.

Absent the establishment of effective and up-to-date policies and procedures for each IT function, Department management has reduced assurance that IT controls have been suitably designed and will be appropriately implemented.

Recommendation: We recommend that Department management establish effective and up-to-date policies and procedures for each IT function identified in the risk assessment survey.

Finding 10: IT Access Controls

Effective IT access controls are intended to prevent or detect inappropriate access to IT resources and to protect the confidentiality, integrity, and availability of data. Effective access controls include provisions to timely remove employee access privileges when access is no longer required. Department policies and procedures specified that the Department, Division of Information Technology Services, was to deactivate user access privileges to the Department's network within 48 hours of receiving notice of an employee separating from Department employment. Network access was required for users to access MatrixCare and UltraCare.

In our report No. 2014-007, finding No. 11, we noted that the Department did not always timely remove terminated employees' access to the Department's network and UltraCare. As part of our audit follow-up procedures, we reviewed Department records for 25 employees who separated from Department employment during the period January 2014 through February 2015 to determine whether, as applicable, network, UltraCare, and MatrixCare access privileges had been timely deactivated. Our audit procedures again disclosed that user access privileges were not always timely deactivated. Specifically, we noted that:

- For five of ten employees with user access privileges to the network and UltraCare, 10 to 122 business days (average of 33 business days) had elapsed from the date of employee separation from Department employment to the date network and UltraCare user access privileges were deactivated.
- For five of ten employees with user access privileges to the network and MatrixCare, 9 to 83 business days (average of 35 business days) had elapsed from the date of employee separation from Department employment to the date network and MatrixCare user access privileges were deactivated.

Effective access controls also include provisions to ensure that employees are authorized access to IT resources only as needed to accomplish their job duties. As part of our examination of the appropriateness of security and administration access privileges to the Department's network as of April 2015, we found that one of the Department's ten employees with network administrator access privileges had such privileges although they were not commensurate with the employee's job duties. In addition, we found that 2 of the Department's 11 service accounts with network administrator access privileges were not necessary. Subsequent to our audit inquiry, Department personnel indicated that the access privileges had been deleted for all three accounts.

Delays in deactivating user access privileges upon an employee's separation from Department employment or when access privileges are not needed increase the risk of inappropriate access to IT resources and unauthorized disclosure, modification, or destruction of Department data and IT resources.

Recommendation: To minimize the risk of compromising Department data and IT resources, we again recommend that Department management ensure that all IT access privileges are deactivated immediately upon a user's separation from employment and that all IT access privileges are necessary and commensurate with user job duties.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for the findings included in our report No. 2014-007.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this operational audit from April 2015 through July 2015 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.

This operational audit focused on resident care assessments and collections, Residents' Deposits Trust Fund accounts, and selected information technology (IT) controls. The overall objectives of the audit were:

- To evaluate management's performance in establishing and maintaining internal controls, including controls designed to prevent and detect fraud, waste, and abuse, and in administering assigned responsibilities in accordance with applicable laws, administrative rules, contracts, grant agreements, and guidelines.
- To examine internal controls designed and placed in operation to promote and encourage the achievement of management's control objectives in the categories of compliance, economic and efficient operations, the reliability of records and reports, and the safeguarding of assets, and identify weaknesses in those internal controls.
- To determine whether management had corrected, or was in the process of correcting, all deficiencies disclosed in our report No. 2014-007.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for those programs, activities, or functions included within the scope of the audit, deficiencies in management's internal controls, instances of noncompliance with applicable governing laws, rules, or contracts, and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular transactions, legal compliance matters, records, and controls considered.

As described in more detail below, for those programs, activities, and functions included within the scope of our audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of our audit; obtaining an understanding of the program, activity, or function; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of our audit's findings and conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

Our audit included the selection and examination of transactions and records. Unless otherwise indicated in this report, these transactions and records were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature, does not include a review of all records and actions of agency management, staff, and vendors, and as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting our audit we:

- Obtained an understanding of internal controls and tested key processes related to resident care assessments and collections and Residents' Deposits Trust Fund accounts. Specifically, we:

- Analyzed occupancy rates and resident care reimbursements to evaluate the reasonableness of cost-of-care revenues compared to occupancy rates and verified that Department management was provided timely occupancy rates and revenue reports during the period January 2014 through February 2015.
- From the population of all census records at each facility during the period January 2014 through February 2015, examined Department records for 70 residents (10 at each of the six nursing homes and 10 at the Domiciliary) to determine whether a ledger had been established for the resident in MatrixCare; a complete resident health record was maintained; an annual reevaluation was on file; adequate records existed to demonstrate eligibility, income verification, and Medicaid status; and the resident's admittance was based on statutory requirements.
- Examined documentation related to assessment amounts recorded as due from 70 residents (10 at each of the six nursing homes and 10 at the Domiciliary) during the period January 2014 through February 2015 to determine whether charges were properly assessed, supported, and recorded; the resident's payment classification was properly recorded in the resident ledger; and the collections were timely received.
- Examined documented related to 59 charges incurred during the period January 2014 through February 2015 for supplies or services received by residents (10 each at the Bennett, Jacobson, Lassen, Lopez, and Nininger Nursing Homes and 9 at the Sims Nursing Home) to determine if the charges were evidenced by receipt, supported, timely and accurately recorded in the resident ledgers, and appropriately and timely collected.
- Examined documentation related to 60 pharmacy charges incurred by residents (10 at each of the six nursing homes) during the period January 2014 through February 2015 to determine whether the charges were evidenced by nursing or other resident records, the charges for dispensed pharmaceuticals were posted to the resident's receivable ledger, the delivery of pharmaceuticals was documented, and the appropriate amounts were timely collected.
- Performed inquiries, inspections of selected records, and observations at the nursing homes and the Domiciliary to evaluate the adequacy of actions taken by facility staff to safeguard moneys collected during the period January 2014 through February 2015.
- Analyzed Medicaid and Medicare records at the Department's Central Office to determine whether all amounts billed during the period January 2014 through February 2015 were collected. In addition, examined nurses' census records for January 2015 to determine whether all Medicaid and Medicare payments related to resident-occupied rooms.
- Performed inquiries and inspections of selected documents and records relating to resident account write-offs to determine whether the Department had adequately designed and implemented controls to ensure the appropriate recording of write-offs.
- Evaluated internal controls over Residents' Deposits Trust Fund accounts at all six nursing homes and the Domiciliary and tested the facilities' compliance with the requirements of State law during the period January 2014 through February 2015.
- At each of the nursing homes, examined selected resident trust fund balance sheets and resident fund summaries to determine whether the Department had complied with Medicaid asset limit notification requirements during the period January 2014 through February 2015.
- Examined documentation related to 70 Residents' Deposits Trust Fund deposits (10 at each of the six nursing homes and 10 at the Domiciliary) made during the period January 2014 through February 2015 to determine whether the deposits were accurately recorded to the appropriate resident accounts.
- Examined documentation related to 70 disbursements made by check (10 at each of the six nursing homes and 10 at the Domiciliary) and 70 cash disbursements (10 at each of the

six nursing homes and 10 at the Domiciliary) from the Residents' Deposits Trust Fund during the period January 2014 through February 2015 to determine whether the disbursements were adequately supported and properly authorized.

- Examined documentation related to Residents' Deposits Trust Fund accounts for 104 residents (15 residents at each of the six nursing homes and 14 at the Domiciliary) who were discharged or who deceased during the period January 2014 through February 2015 to determine whether the disbursements were adequately supported, properly authorized, and timely disbursed in accordance with State law.

- Evaluated Department actions taken to correct the findings noted in our report No. 2014-007. Specifically, we:
  - Obtained an understanding of internal controls and evaluated selected contract monitoring processes and documentation related to nursing home service provider contracts at the Bennett and Lopez Nursing Homes to determine whether adequate documentation of contract monitoring efforts was maintained.
  - Examined Department contract monitoring policies and procedures and evaluated whether the policies and procedures appropriately specified contract monitoring documentation retention requirements.
  - Examined Department property records as of January 30, 2015, to determine whether the Department ensured that all attractive items were appropriately identified and tracked and whether all tangible personal property was properly accounted for during the physical inventory process.
  - Examined Department policies and procedures and capital asset records for the period January 2014 through February 2015 to determine whether the policies and procedures facilitated the maintenance of adequate and accurate capital asset subsidiary records and whether capital assets were reported in accordance with applicable requirements.
  - Examined Florida Accounting Information Resource Subsystem records for the 2013-14 fiscal year to determine whether the Department properly recorded activities of the Residents' Deposits Trust Fund in accordance with generally accepted accounting principles.
  - Examined Department records for the 2013 and 2014 calendar years to determine whether the Department timely prepared and submitted reports detailing account collection and write-off activities as specified by State law.
  - Examined Department records for 25 employees who separated from Department employment during the period January 2014 through February 2015 to determine whether, as applicable, network, UltraCare, MatrixCare, and Point of Care Program access privileges were timely deactivated. In addition, examined security and administration access privileges to the Department's network as of April 2015 to determine whether the access privileges were necessary and commensurate with employee job duties.

- Obtained an understanding of selected IT controls, assessed the risks of those controls, evaluated whether selected general IT controls were in place, and tested the effectiveness of the controls. Specifically, we:
  - Performed inquiries and inspections of documents and records to evaluate the Department's IT security policies and procedures and determine whether the Department had established appropriate general IT controls related to the network, shared drives, UltraCare and Matrix Care, and other critical IT resources. Additionally, determined whether the Department had established appropriate entitywide IT policies and procedures.
  - Performed inquiries and inspections of documents and records to evaluate the adequacy of the Department's IT risk assessment, including related policies and procedures, and to

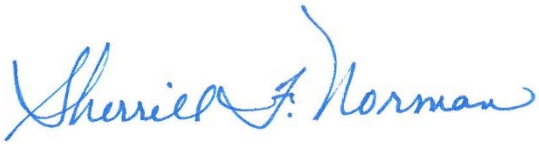
determine whether the Department had established an effective framework and continuous cycle of activity for assessing risk.

- Performed inquiries and inspections of documents and records supporting the Department's security awareness program to determine whether the Department had established an appropriate security awareness training program. In addition, examined Department records for all employees with access to the Department's network as of April 2, 2015, to determine whether the employees timely completed security awareness training and if all Division of Information Technology Services employees received periodic retraining.
- Performed inquiries, inspected documents, and conducted observations to evaluate the physical and environmental security over critical computer infrastructure at the Largo Central Office, Lopez Nursing Home, and Sims Nursing Home. Also, evaluated whether the Department had established appropriate physical and environmental controls at these locations.
- Performed inquiries and inspections of agreements and procedures for monitoring third parties and determined whether third parties were required to establish appropriate controls, including those related to background checks, security awareness training, minimum performance, business continuity and recovery plans, and remedies for noncompliance.
- Performed inquiries and inspections of documents supporting the Department's backup, recovery, and continuity of operations plans and evaluated the sufficiency of such plans.
- Performed inquiries and inspections of documents and evaluated the Department's network configurations including network diagrams, equipment lists, and settings to determine the adequacy of the Department's network configuration controls.

- Observed, documented, and evaluated the effectiveness of selected Department processes and procedures for:
  - Budgetary and cash management.
  - Purchasing.
  - The assignment and use of motor vehicles. Department motor vehicle acquisition costs totaled $291,492 during the period January 2014 through February 2015.
  - The administration of purchasing cards in accordance with applicable State guidelines. As of February 25, 2015, the Department had 151 active purchasing cards.
  - The acquisition, assignment, and use of wireless devices with related usage costs totaling $39,640 during the period January 2014 through February 2015.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

AUTHORITY

Section 11.45, Florida Statutes, requires that the Auditor General conduct an operational audit of each State agency on a periodic basis. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our operational audit.



Sherrill F. Norman, CPA
Auditor General

State of Florida
DEPARTMENT OF VETERANS' AFFAIRS
Office of the Executive Director
11351 Ulmerton Road, #311-K
Largo, FL 33778-1630
Phone: (727) 518-3202 Fax: (727) 518-3403
www.FloridaVets.org

Mike Prendergast
Executive Director

Rick Scott
Governor
Pam Bondi
Attorney General
Jeff Atwater
Chief Financial Officer
Adam Putnam
Commissioner of Agriculture

28 October 2015

Ms. Sherrill F. Norman, Auditor General
State of Florida Auditor General
111 West Madison Street
Tallahassee FL 32399-1450

Dear Ms. Norman:

This letter is in response to your letter dated 28 September 2015, outlining the findings from your 2015 Operational Audit of the Florida Department of Veterans' Affairs (FDVA). Pursuant to Section 11.45(4)(d), Florida Statutes, we are providing our responses to the preliminary and tentative Operational Audit findings and recommendations related to resident care assessments and collections, Residents' Deposits Trust Fund accounts, and selected information technology controls.

FDVA has been proactive in making improvements since the guidance provided by the Auditor General's Operational Audit report issued in August 2013. The agency strives for excellence in the operational processes and appreciates your efforts in assisting us in further improving our operations.

On behalf of FDVA I would like to thank your staff for their professionalism and expertise during the audit process. If you have any questions, please contact the Office of Inspector General at 727-518-3202 extension 5570.

Sincerely,

Mike Prendergast

Mike Prendergast
Colonel, USA, Retired
Executive Director

"Honoring those who served U.S."

Finding No. 1: Collection Safeguards

- Restrictive endorsement of collections - the agency's policies and procedures did not specify the employee position responsible for endorsing checks received at the nursing homes and Domiciliary that were not addressed to a resident. At Lopez, Nininger, and Sims Nursing Homes, non-resident checks were not restrictively endorsed at the point and time of receipt.
- Transfer of custodial responsibility - Bennett, Lopez, and Nininger Nursing Home staff did not document the transfer of collections from one employee to another. The agency's policies and procedures did not provide an appropriate agency wide document to track the transfer of funds from one employee to another.
- Records reconciliation - Nininger Nursing Home staff did not reconcile pre-numbered collection receipts to the Cash Receipt Register used to prepare bank deposits.

Agency Response:
The agency concurs that the Homes did not consistently practice restricted endorsement of collections, transfer of custodial responsibility, and records reconciliation.

Corrective Action Plan:
An in-service training was held on 21 October 2015, for the Homes Business Office personnel to discuss audit finding #1, Collection Safeguards. The Homes Administrators, Business Managers, Accountant II's and Receptionists discussed, and agreed to change standards and procedures #2207 so that all the homes would conform to the same standards and procedures. The agreed upon changes to standards and procedure #2207 will be updated by the Accounting Specialist and will be posted under the Veteran's Homes " Standard Operating Procedures."
The Business Manager provides oversight to the Accountant II and Receptionist in the Homes business office. The Business Manager is responsible for ensuring the Business Office staff complies with the standards and procedures #2207 requirement of restrictively endorsing checks at point of receipt; establishing and maintaining the chain of custody between employees; and the receipt, recording, depositing and timely reconciling of bank deposit records.
Quarterly Audits will be performed on each of the Homes by the Homes' Department Professional Accountant Specialist to ensure standards and procedures #2207 endorsement requirements; chain of custody of collections between employees; and the receipt, recording, depositing and reconciling of funds are being followed.

Finding No. 2: Annual Financial Update

The Domiciliary Annual Financial Update Tracking log disclosed that as of 05 May 2015, 15 of 134 residents had not returned a completed Financial Data Update form and 64 residents had returned completed forms from 1 to 68 days (an average of 22 days) after the February 15th deadline.

Agency Response:
The agency concurs that not all of the residents' Annual Financial Updates were completed by the February 15th deadline.

Corrective Action Plan:
An in-service training was held on 21 October 2015, for all of the Homes Business Office personnel to discuss audit finding #2, Annual Financial Update. The Homes Administrators, Business Managers, Accountant II's and Receptionists discussed, and agreed upon the importance of continuing to promote timely receipt of the Financial Data forms and supporting documentation as required by standards and procedures #2200. The Professional Accountant Specialist will post the standards and procedures #2200 under the Veteran's Homes "Standard Operating Procedure."
The Business Manager provides oversight to the Accountant II and Receptionist in the Homes business office. The Business Manager is responsible for ensuring the business office staff complies with standards and procedures #2200 yearly requirement of requesting financial information and supporting documentation from the facilities residents, family members or legal guardians.
Yearly Audits will be performed on each of the Homes by the Homes' Department Professional Accountant Specialist to ensure timely receipt of the required financial update forms and supporting documentation.

Finding No. 3: Residents' Deposits Trust Fund Policies and Procedures

- The Sims Nursing Home Administrator, who resigned on 16 September 2013, was not removed as an authorized check signer on one account until 25 February 2015. The Deputy Executive Director of the agency was listed as an authorized signer for one bank account, which did not appear to be necessary and in accordance with agency policies and procedures.
- Sims and Nininger Nursing Homes did not always obtain written authorizations for disbursements nor the signature of two witnesses to support resident's verbal authorizations for disbursements in accordance with agency policies and procedures.

Agency Response:
The agency concurs that the Homes did not consistently adhere to agency policy and procedure on the administration of Residents' Deposits Trust Fund accounts.

Corrective Action Plan:
An in-service training was held on 21 October 2015, for the Homes Business Office personnel to discuss audit finding #3, Residents's Deposits Trust Fund Policies and Procedures. The Homes Administrators, Business Managers, Accountant II's and Receptionists discussed, and agreed upon changes to standards and procedures #2205 and #2206 which will be updated by the Accounting Specialist and posted under the Veteran's Homes "Standard Operating Procedures."
The Business Manager provides oversight to the Accountant II and Receptionist in the facility's business office. The Business Manager and Facility's Administrator are responsible for standards and procedures #2205 Safeguarding Facility and Resident Funds specifically maintaining valid signatures and bank signature cards at all times. The Business Manager is responsible for ensuring the Business office staff complies with standards and procedures #2206, Withdrawal of Resident Trust Fund Monies, specifically the requirement for two witnesses to support each verbal authorization for a resident disbursement.

Quarterly Audits will be performed on each of the Homes by the Homes' Department Professional Accountant Specialist to ensure standards and procedures #2206, Withdrawal of Resident Trust Fund Monies, are being followed, specifically the requirement for two witnesses to support each verbal authorization for a resident disbursement. The Professional Accountant Specialist will also perform quarterly audits on the bank signature cards and validate signatures for each facility per standards and procedures #2205, Safeguarding Facility and Resident Funds.

Finding No. 4: Medicaid Asset Limit

- Bennett and Sims Nursing Homes staff could not provide documentation demonstrating that a spending plan, and the potential for becoming ineligible for Medicaid, had always been discussed with the applicable resident (or their representative) when the Resident Trust Fund account balances were near or at $1,500.
- Bennett and Sims Nursing Homes staff could not provide documentation that the agency always sent a letter notifying the applicable resident or their representative that the Medicaid asset limit was being approached when the Resident Trust Fund account balances reached $1,800.
- The Medicaid asset limit policies and procedures did not specify the anticipated costs that could be factored into, or the resources that could be excluded from, the determination of a Resident Trust Fund account balance for Medicaid asset limit purposes.

Agency Response:
The agency concurs that the Medicaid participating residents were not consistently notified in a proper and timely manner of potential Medicaid program ineligibility in accordance to agency policies and procedures. In addition, the agency policies and procedures do not specify the anticipated costs that may be factored into, and the resources that may be excluded from, the determination of the Resident Trust Fund account balance for the Medicaid asset limit.

Corrective Action Plan:
An in-service training was held on 21 October 2015, for the Homes Business Office personnel to discuss audit finding #4, Medicaid Asset limit. The Administrator's, Business Manager's and Accountant II's discussed, and agreed to further enhance standards and procedure #2206-K. The changes to standards and procedures #2206-K will be updated by the Accounting Specialist and will be posted under the Veteran's Homes "Standard Operating Procedures."
The Business Manager provides oversight to the Accountant II in the facility business office. The Business Manager is responsible for ensuring that the Business Office staff compiles with the standards and procedures #2206-K requirement notifying residents properly and timely of potential Medicaid Program ineligibly.
The Business Office Manager will run a Resident Trust Fund account balance report on a monthly basis after Room and Board costs are transferred. Additionally:

- If a Medicaid resident's account balance is near or at $1,500, the Activities personnel, the Social Worker, and the Business Manager will coordinate a spending plan based on the resident's needs and will communicate to the resident and/or the resident's representative. The information will be documented in MATRIXCare by the Business Manager and in Care Plan by the Social Worker.
- If a Medicaid resident's account balance is within $200 of the $1,800 threshold, a

notification letter will be sent to the resident and/or the resident's representative informing them that the account balance may exceed the Medicaid asset limit ($2,000) and may affect their eligibility. The information will be documented in MATRIXCare.

- If a Medicaid resident's account balance exceeds $2,000, the Business Manager will send a "Client Discharge/Change Notice" to the Department of Children and Families to advise them of the status of the resident. The information will be documented in MATRIXCare.

On a monthly basis the Business Manager or/Accountant II will provide to the Professional Accountant Specialist a Resident Trust Fund Medicaid Asset Limit report on account balances greater than $1,900. The Professional Accounting Specialist will follow up with the business office on any Medicaid ineligible resident.

Finding No. 5: Resident Account Close-Out Process

For 2 of 15 accounts examined at the Nininger Nursing Home, staff disbursed resident funds, totaling $50 and $108, 35 and 49 days, after the former resident's discharge or death.

Agency Response:
The agency concurs that resident funds were not consistently closed out within thirty (30) days for discharged/expired residents in accordance to Florida Statute 400.022(1)(h)(4), Residents' Rights.

Corrective Action Plan:
An in-service training was held on 21 October 2015, for the Homes Business Office personnel to discuss audit finding #5, Resident Account Close-Out Process. The Administrators, Business Managers and Accountant II's discussed, and agreed on the importance of following standards and procedures #2206-F, Death and Discharge of Resident Monies in Resident Trust Fund.
The Business Manager provides oversight to the Accountant II in the facility's business office. The Business Manager is responsible for ensuring that the business office staff complies with standards and procedures #2206-F requirement of a timely audit on all discharged or expired resident trust fund accounts. Any refunds due to the resident and or beneficiary are due within 30 days by the facility.
Quarterly audits will be performed at each of the facilities by the Homes' Department professional Accountant Specialist to ensure standards and procedure #2206-F, Death and Discharge of Residents Monies is being followed.

Finding No. 6: Risk Management Program

The Department had not established a risk management program and categorized IT risks in accordance with governing rules. In addition, Department monitoring of IT controls need improvement.

Agency Response:
We concur that the agency has not implemented a documented and approved risk management program that categorizes IT risks in accordance to FIPS.

Corrective Action Plan:
The areas identified in the audit were already annotated in the Risk Assessment Survey as areas

of improvement with a completion within twelve months. The Chief Information Officer and Information System Management are scheduled to complete the Risk Management Framework Training provided by Florida Agency for State Technology the week of 02 November 2015. Additionally, the Department will enhance monitoring of IT controls.

Finding No. 7: Continuity of Operations and Disaster Recovery

The Agency's Continuity of Operations Plan (COOP) and certain backup and recovery policies and procedures need enhancement.

Agency Response:
We concur that the agency has not approved an updated COOP that includes enhanced backup location provisions, establishes policies and procedures for backing up and recovering all critical IT systems and data, and documents recovery test results.

Corrective Action Plan:
The Agency is currently reviewing and updating the COOP and Disaster Recovery Plans (DRP) to reflect the current environment. The updated documents will go through the management approval process and will be completed by 01 January 2016.
The agency currently uses Data Protection Manager that is mirrored to the off-site location at Land O'Lakes. The IT division will purchase a Tape Drive within the next budget cycle to complete a monthly backup of the following data for archiving purposes: Microsoft Exchange, File Server, ULTRACare, and potentially VBOLTS. These tapes will be kept for seven years.
The IT division will establish a backup policy and procedure concerning backup and recovery that will include a documented recovery test plan. The test results will be annotated and kept in the ServiceDesk application.
The agency is accepting the risk of the off-site location being within 50 miles from the primary location. A letter to that affect will be drafted and kept with the COOP and DRP plan by 01 January 2016.

Finding No. 8: Evaluation of Service Auditor's Reports

The agency had not requested or reviewed the service auditor's reports on the effectiveness of the controls established by the Department's vendor for MatrixCare, nor established policies and procedures for monitoring third party IT service provider compliance with the agency's requirements.

Agency Response:
We concur the agency has not requested, obtained, or reviewed the service auditor's reports as well as established a policy and procedure for monitoring third party IT service providers.

Corrective Action Plan:
The IT department will establish a policy and procedure for monitoring third-party IT service providers to ensure compliance with agency requirements. These policies and procedures will be in place by 30 June 2016. The ServiceDesk application that the IT department uses will provide additional monitoring tools by annotating trouble tickets pertaining to the third party applications. The implementation of the ServiceDesk monitoring of trouble tickets has been

completed.

Finding No. 9: IT Policies and Procedures

The risk assessment survey completed by the agency identified that the agency had not:

- Kept selected agency security documentation up to date.
- Documented data security policies and procedures.
- Created a system security plan.
- Documented secure coding policies.
- Documented device configuration standards and,
- Documented network security procedures for perimeter control and secure wireless implementation.

Agency Response:

We concur that the agency has not establish effective and up to date policies and procedures for each IT function identified in the risk assessment survey.

Corrective Action Plan:

The IT department is in the process of updating all IT policies and procedures as well as creating a system security and risk management plan. The agency will insert the device configuration standards as part of the updating of the IT Policies and Procedures. All IT Policies and Procedures will be updated and/or created within the next 12 months.
The agency does not conduct any database programming thus does not need secure coding policies. The agency is implementing a new perimeter control system that will provide monitoring and analyzing capabilities. The projected date of completion for this system is 01 January 2016.

Finding No. 10: IT Access Controls

The agency did not always timely deactivate IT user access privileges upon an employee's separation from the agency employment. Additionally, the agency did not always ensure that network access privileges were necessary

Agency Response:

We concur that the agency did not consistently deactivate IT access privileges immediately upon a user's separation from employment; and that all IT access privileges were not necessary and commensurate with user job duties.

Corrective Action Plan:

Upon the department, directorate, or activities notification of an employee leaving the agency, the employee out-processing checklist is initiated. Included on this departure checklist will be the requirement to clear network access with the IT Directorate. The IT Directorate currently requires managers to complete a "Network Access/Termination Form" that is located on the agency's intranet. It is currently the manager's responsibility to identify what access their employees have to what applications. This form will then be automatically submitted into the

helpdesk ticketing system where it is assigned and confirmed completion of the requested tasks. The FDVA Human Resources Office will revise its out-processing checklist to add this requirement. The projected update to the policy will be 01 January 2016.