FLORIDA AGENCY FOR HEALTH CARE ADMINISTRATION

Office of the Inspector General
Internal Audit

Report No. 13-15
November 2013

Review of the Agency's Data Exchange MOU with DHSMV

EXECUTIVE SUMMARY

At the request of the Department of Highway Safety and Motor Vehicles (DHSMV), Internal Audit conducted a review of the Agency for Health Care Administration's (Agency) compliance with MOU-HSMV 180-12. This Memorandum of Understanding (MOU) establishes the conditions under which DHSMV provides electronic access to driver license and motor vehicle data to the Agency.

In a limited review of the Agency's use of data obtained through this agreement, it appears users obtained data in accordance with the MOU. However, the Agency does not have documentation or processes in place to address compliance for most of the MOU requirements. We have identified opportunities for improvements in documentation, processes, policy/procedure and form development and training. The Findings and Recommendations section of this report provides details of our evaluation results.

SCOPE, OBJECTIVES, AND METHODOLOGY

The scope of this audit included the Office of Inspector General's Investigations Unit (Investigations) and the Division of Operation's Bureau of Support Services (Support Services); and their use of DHSMV's Driver and Vehicle Express (DAVE) system. The time period reviewed was from September 1, 2011 to August 31, 2012, with a limited review of activities outside the identified time period.

The objective was to determine whether the Agency has appropriate internal controls to protect personal data exchanged under the MOU from unauthorized access, distribution, use, modification or disclosure.

To accomplish our objectives, we reviewed applicable laws, and regulations; interviewed appropriate Agency staff; and reviewed policies, procedures, MOUs and related documents.

BACKGROUND

According to Section 322.02(2), Florida Statutes (F.S), the DHSMV is responsible for the administration of the state's drivers' licenses function. As part of this function, DHSMV administers the DAVE system. DAVE is a source of title and registration data on all vehicles owned or registered to a driver or business in Florida. DAVE contains confidential personal information that is covered under federal and state laws listed in the following paragraphs.

Title 18, Chapter 123 –of the U.S. Code, Section 2721 states:

> (a) In General.—A State department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity:
> (1) personal information, as defined in 18 U.S.C. 2725(3)[1], about any individual obtained by the department in connection with a motor vehicle record, except as provided in subsection (b) of this section; or
> (2) highly restricted personal information, as defined in 18 U.S.C. 2725(4) [2], about any individual obtained by the department in connection with a motor vehicle record, without the express consent of the person to whom such information applies, except uses permitted in subsections (b)(1), (b)(4), (b)(6), and (b)(9): **Provided**, That subsection (a)(2) shall not in any way affect the use of organ donation information on an individual's driver's license or affect the administration of organ donation initiatives in the States.

Section 119.0712(2)(b), F.S; states:

> Personal information, including highly restricted personal information as defined in 18 U.S.C. s. 2725, contained in a motor vehicle record is confidential pursuant to the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. ss. 2721 et seq. Such information may be released only as authorized by that act; however, information received pursuant to that act may not be used for mass commercial solicitation of clients for litigation against motor vehicle dealers.

The statutes also authorize DHSMV to "enter into reciprocal driver's license agreements with other jurisdictions within the United States."[3] Any agency that enters into a MOU with DHSMV for access to DAVE is responsible for protecting confidential data. Some examples of confidential data in DAVE are: name, address, Social Security Number and Driver Identification Number.

To ensure compliance with laws and agreements, DHSMV requires the Agency to perform four types of monitoring:

- Ongoing monitoring
- Quarterly reviews
- Annual Affirmation Statement
- Attestation - every three years

[1] "personal information" means information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status.
[2] "highly restricted personal information" means an individual's photograph or image, social security number, medical or disability information;
[3] Section 322.02(4), F.S.

On October 23, 2008, DHSMV approved a Data Exchange MOU with the Agency. This MOU covers the purposes and conditions for access to the DAVE database. Specific to this MOU, the Agency requested access to vehicle registrations, current addresses, registered owners, tag number and lien holder names to:

> Conduct Florida Medicaid investigations per 409.913 and 20.055 Florida Statutes. The data provided through DAVE will assist in verifying Medicaid recipients, providers and other Medicaid entities.

In November 2008, the Agency faxed Access Authorization Requests to DHSMV for three employees from Investigations. DHSMV subsequently approved their access.

The Agency sent three additional access requests to DHSMV in May 2009. Access was requested to assist Support Services staff in monitoring Agency parking for improper use of handicapped and visitor spaces. Upon request, they will also monitor vehicles in areas not marked for parking. Support Services staff received DAVE access in September 2009.

On September 6, 2011, DHSMV approved a new Data Exchange MOU with the Agency. The 2011 MOU's purpose was identical to that of the 2008 MOU.

On October 9, 2012, DHSMV sent a letter to the DAVE Administrator requesting the Agency to submit an attestation within 180 days. The letter stated the attestation may be performed by the Agency's "internal auditor or inspector general" since the Agency is a governmental entity. According to DHSMV's letter, the Agency was randomly chosen to submit the requested attestation. In March 2013, the Agency requested a two-week extension from the original deadline of April 9, 2013. DHSMV approved the request. On April 22, 2013, the Agency sent the requested attestation and supporting documentation to DHSMV.

INDEPENDENCE

Pursuant to Section 20.055, F.S., this engagement was performed under the direction of the Audit Director and conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* (*Standards*) as established by the Institute of Internal Auditors. These *Standards* require us to be organizationally independent and objective in the performance of our work. However, since Investigations and Internal Audit both report organizationally to the Office of Inspector General, we are required to disclose this potential impairment to our independence and objectivity. Except for the noted impairment, we have adhered to the *Standards* of our profession in conducting this engagement.

FINDINGS, RECOMMENDATIONS AND MANAGEMENT'S RESPONSES

Finding 1: Policies and Procedures

Section V.G. of the MOU, Agency agreed that: "By signing the MOU, the representatives of the Providing Agency and Requesting Party, on behalf of the respective Parties attest that their respective agency procedures will ensure the confidentiality of the information exchanged will be maintained."

When we asked Investigations about policies and procedures, we were told there were no written policies or procedures. Investigations, where the DAVE Administrator is located, has not addressed this requirement of the MOU.

Having policies and procedures for the use of DAVE will not only ensure compliance with this specific requirement of the MOU but make clear to all DAVE users what their responsibilities are for all DAVE requirements.

Recommendation

The Investigations Unit should be responsible for development of policies and procedures to address the use of DAVE and MOU compliance requirements.

Management Responses

1. Investigations will develop policies and procedures addressing the use of DAVE by Investigations staff and compliance with MOU requirements.
2. Support Services will assist in drafting procedures as needed.

Finding 2: MOU's Purpose

According to Section IV.B.6 of the MOU, the Agency agreed to: "Use the information received from the Providing Agency only for the purposes authorized by this agreement."

In 2008, when the Agency signed an MOU with the DHSMV, the listed purpose for access was Medicaid investigations. Three Investigations' employees were given access to DAVE. When three Support Services employees were added in 2009, the MOU was not amended to cover the additional purpose of monitoring Agency parking for improper use of handicapped and visitor spaces. In 2011, when the Agency renewed its MOU with DHSMV, it did not update the purpose to include the reason for Support Services access to DAVE.

Even though the Agency's MOU does not fully address why its staff accesses DAVE, DHSMV appeared to have some knowledge of Support Services' need to access DAVE. DHSMV corresponded with the Agency before granting access to Support Services' staff. At some point, the Agency prepared a modification to the MOU; however, DHSMV did not have any documentation to support the Agency's request to amend the MOU.

Because the MOU has not been updated, it could appear that some of the Agency users are obtaining information from DAVE that might be considered unauthorized.

Recommendation

Investigations should amend the Agency's MOU with DHSMV to include the purpose for Support Services' access.

Management Response

1. The MOU will be updated with Support Services' reason for DAVE access and routed to the Secretary for signature.
2. Support Services will assist in drafting the portion of the MOU to include monitoring of Agency parking for improper use of handicapped and visitor spaces and also parking in no-parking areas as needed.

Finding 3: Supporting Documentation

The attestation, requested by DHSMV in 2012, required a review of users' accesses to determine if users are "using the data in an appropriate manner." We obtained one year of users' accesses (9/1/11 to 8/31/12) and requested that the users review the reports and provide documentation for their accesses. None of the users had any documentation to support why they accessed license or tag information.

Because there is no documentation to support Agency users' accesses, it might appear that users accessed information for the wrong purpose. Since this project began, Investigations has begun logging their accesses. Maintaining a log not only documents Agency employees' purpose for accesses, but should also provide for more efficient and effective reviews.

Recommendations

1. Investigations should formally document its log process in written procedures.
2. Support Services should create a log to document its access to DAVE. The log process should also be formally documented by Investigations in written procedures.

Management Responses

1. Investigations has created a log to document its access to DAVE. Investigations will formally develop written procedures documenting the log process.
2. Support Services has created a log to document its access to DAVE. The log is password protected. Facilities staff and the bureau chief have access to the password. Support Services will assist in drafting the portion of the procedures that pertain to the log as needed.

Finding 4: Confidentiality and Security

Sections IV.B.7 and V.C. of the MOU address protecting and maintaining the confidentiality and security of driver license and motor vehicle information.[4]

During the audit period, Investigations stored case files containing confidential DAVE information in Investigator and Administrative offices; staff doors were not always locked. After this project started, Investigations began storing completed files in a locked room and locking investigators' offices after hours. We also noted some staff, responsible for the files that contain information from DAVE, were not aware of the security requirements related to DAVE information.

According to interviews with Support Services, staff do not normally print DAVE information. They may write down the name of the tag owner for communication purposes. If they write anything on paper, they ensure the paper is shredded. During a recent discussion, Support Services disclosed they keep a list of names of Agency staff on their share drive who have not complied with parking policies.

Neither Investigations nor Support Services have any documented procedures on the use of DAVE. The lack of written policies/procedures addressing the MOU requirements and training for all staff that have access to DAVE information has put the Agency at risk. Anyone who comes into the Investigations area could potentially view confidential information if the files are not secured within individual offices. Anyone with access to Support Services share drive could view the list of Agency staff.

Recommendations

1. Investigations should document and implement procedures to ensure DAVE users and any associated personnel understand the confidentiality/security of data obtained from DAVE.
2. All Investigations and Support Services (who handle DAVE information) staff should be trained in the handling of DAVE information.
3. Any DAVE-related information in Investigations should be contained where it is not accessible to any person coming into the common areas.
4. Support Services should ensure any DAVE-related information stored on a shared drive is accessible only to DAVE-authorized staff.

Management Responses

1. Investigations will document and implement procedures ensuring DAVE users within the Investigations Unit and any associated Investigations personnel understand the confidentiality/security of data obtained from DAVE.
2. Investigations staff have received training. Investigations will continue to participate in training required for DAVE use.

[4] "Protect and maintain the confidentiality and security of driver license and/or motor vehicle information received from the Providing Agency in accordance with this MOU and applicable state and federal law." (IV.B.7) and "Access to the information exchanged will be protected in such a way that unauthorized persons cannot review or retrieve the information." (V.C.)

Users in Support Services have received training. Support Services will continue to participate in training required for DAVE use.

3. Investigations has implemented storage of all DAVE-related information in closed and locked offices. The data is not accessible to any person coming into the common areas.
4. Support Services has created a log to document its access to DAVE. The log is password protected. Facilities staff and the bureau chief have access to the password.

Finding 5: Access Terminations and Quarterly Reviews

Section IV.B.9 of the MOU requires the Agency to:

> Update user access permissions upon termination or reassignment of users within 5 working days and immediately update user access permissions upon discovery of negligent, improper, or unauthorized use or dissemination of information. Conduct quarterly quality control reviews to ensure all current users are appropriately authorized.

The Agency has terminated two users' access permissions. One user's access permission was not terminated within the five working days allowed by the MOU. This employee's last day with Investigations was December 9, 2010; she left the agency on May 29, 2012. Her access permission was not terminated until February 1, 2013. The other user's access permission was terminated timely. His last day of employment with the Agency was January 31, 2013 and his access permission was terminated on February 1, 2013.

We were unable to find documentation to support the Agency's stance that quarterly reviews had been performed. Further evidence of non-review is listed in the above paragraph when an employee was authorized for DAVE use for over a year after leaving the Agency.

The Agency does not have a process or maintain documentation to ensure compliance with MOU requirements for timely terminations and quarterly reviews of users' access permissions. Although Support Services and Investigations use the Agency's employee separation checklist, this checklist does not address application or system access permission termination.

The Agency's Division of Information Technology has a Network Access Form (NAF) that addresses access to **internal** applications. There are forms for New User/Change/Terminate and for User Transfer/Promotion. DAVE is an **external** application that would not be covered under the Agency's NAF forms.

Users who leave the Agency or are reassigned might access DAVE inappropriately if their access permissions are not terminated promptly. Any user, whether current or not, could access DAVE for purposes other than those allowed in the MOU.

Recommendations

1. Investigations should document and ensure user access permissions are terminated in compliance with the MOU requirements. The DAVE Administrator should be responsible for maintaining all documentation for user access permissions.
2. The Inspector General should appoint a staff person (Staff Person) independent of the DAVE process to conduct the quarterly reviews. Instructions and the quarterly quality control review form are located at: https://idave.flhsmv.gov/message_center.html.
3. The Staff Person should formally document and conduct quarterly reviews of users' authorizations. This person should develop desk procedures to address responsibilities addressed in this report.
4. The Bureau of Human Resources should modify the "Employee Separation Checklist" to include termination of the employee's access permissions to all systems or applications, whether internal or external. The Checklist should address any type of separation for the employee (e.g. transfer, promotion, demotion, termination, etc.).

Management Responses

1. a) Investigations will ensure user access permissions for DAVE Users in Investigations will be terminated in compliance with the MOU requirements for staff who leave the office or if access is no longer required.
   b) Support Services will ensure it requests termination of DAVE access for staff who leave the bureau or if access is no longer required.
   c) The DAVE administrator will maintain all documentation for user access permissions and terminations.
2. The Inspector General has appointed a direct reporting person independent of the DAVE process to conduct the quarterly reviews. This appointment will be formalized by an appointment memorandum.
3. The appointed staff person within the Office of Inspector General who is independent of the DAVE process will work with the Inspector General to develop desk procedures for quarterly usage reviews.
4. The Bureau of Human Resources made changes to the Employee Separation Checklist to include a space for the supervisor to check that internal and external systems access has been terminated.

Finding 6: Sharing of Confidential Information

Section V.A. of the MOU states:

> Information exchanged will not be used for any purposes not specifically authorized by this agreement. Unauthorized use includes, but is not limited to, queries not related to a legitimate business purpose, personal use, and the dissemination, sharing, copying or passing of this information to unauthorized persons.

Staff from Investigations and Support Services access DAVE and obtain information which is defined as "confidential" under the terms of the MOU between the Agency and DHSMV.

Support Services staff access DAVE to verify vehicle tag information. They do not normally print any information; if they print the tag number or name of tag owner, they shred the information.

However, Investigations' staff use the database to verify Medicaid provider, Medicaid recipient and employee information; this information is printed and given to the requesting Investigator. The information then becomes part of the investigative file. All investigative files are available for public records requests, unless they meet the requirements of either Section 119.071(2)(g)1.a. or Section 20.055(5)(b), F.S.

Investigations does not have any written procedures addressing public records requests or the confidentiality of DAVE information. Anyone requesting public record access to investigative files might view DAVE information.

Recommendations

1. Investigations should document and implement procedures addressing public records requests. The procedures should include specific instructions on how to document confidential information, including DAVE information, in investigative files.
2. All Investigations' staff should be trained about public records and understand the confidentiality of DAVE information, whether they access DAVE or not.

Management Responses

1. Investigations will document and implement procedures addressing public record requests for requests received by the Investigations Unit. The procedures will include specific instructions on how to document confidential information, including DAVE information, in investigative files.
2. All investigations' staff will be trained about public records and understand the confidentiality of DAVE information.

Finding 7: Confidentiality Acknowledgements

Section V.D. of the MOU requires that:

> All personnel with access to the information exchanged under the terms of this agreement will be instructed of, and acknowledge their understanding of, the confidential nature of the information. These acknowledgements must be maintained in a current status by the Requesting Party.

The Agency, who is the Requesting Party, does not have any documentation of DAVE users' acknowledgements of confidentiality requirements or that staff was instructed about the confidentiality of DAVE information; however Agency users are required to acknowledge "All data contained within the MDAVE system is sensitive and privileged information and shall be handled accordingly…." each time they log into DAVE. The identified users during the audit period stated that they had no training. In February of this year, DHSMV provided Internal

Audit with a Confidential Acknowledgement form that they recently developed to assist Requesting Parties in documenting users' acknowledgements.

The Agency did not have a process or maintain documentation to ensure compliance with the MOU requirement about confidentiality acknowledgements. Because staff were not trained and did not sign an acknowledgement about confidentiality, there is an increased risk staff might inadvertently share confidential DAVE information.

Recommendation

All current DAVE users and any staff with access to DAVE information should sign DHSMV's Confidentiality Acknowledgement forms. These forms should be maintained in a central file maintained by the DAVE Administrator for documentation purposes.

Management Responses

1. Investigations staff with access to DAVE will sign DHSMV's Confidentiality Acknowledgement Forms and provide them to the DAVE Administrator.
2. Support Services staff with access to DAVE will sign DHSMV's Confidentiality Acknowledgement Forms and provide them to the DAVE Administrator.
3. The DAVE administrator will maintain all DHSMV's Confidentiality Acknowledgement Forms for Support Services and Investigations.

Finding 8: Criminal Sanctions Acknowledgement

Section V.E. of the MOU requires that:

> All personnel with access to the information will be instructed of, and acknowledge their understanding of, the criminal sanctions specified in state law for unauthorized use of the data. These acknowledgements must be maintained in a current status by the Requesting Party.

The Agency, who is the Requesting Party, does not have any documentation of DAVE users' acknowledgements or that staff was instructed about the criminal sanctions related to misuse of DAVE information; however, Agency users are required to acknowledge "Unauthorized use…of MDAVE information…could result in civil proceedings against the offending agency and/or criminal proceedings against any user or other person involved." The identified users during the audit period stated that they had no training. In February of this year, DHSMV provided Internal Audit with a Criminal Sanctions Acknowledgement form that they recently developed to assist Requesting Parties in documenting users' acknowledgements.

The Agency did not have a process or maintain documentation to ensure compliance with the MOU requirement about criminal sanctions acknowledgements. Because staff were not trained and did not sign an acknowledgement about criminal sanctions, there is an increased risk staff might inadvertently share confidential DAVE information.

Recommendation

All current DAVE users and any staff with access to DAVE information should sign DHSMV's Criminal Sanctions Acknowledgement forms. These forms should be maintained in a central file maintained by the DAVE Administrator for documentation purposes.

Management Responses

1. Investigations staff with access to DAVE will sign DHSMV's Criminal Sanctions Acknowledgement Forms and provide them to the DAVE Administrator.
2. Support Services staff with access to DAVE will sign DHSMV's Criminal Sanctions Acknowledgement Forms and provide them to the DAVE Administrator.
3. The DAVE administrator will maintain all DHSMV's Criminal Sanctions Acknowledgement Forms for Support Services and Investigations.

Finding 9: On-going Monitoring and Annual Affirmation Statement

According to Section V.F. of the MOU, "All access to the information must be monitored on an on-going basis by the Requesting Party. In addition, the Requesting Party must complete an annual audit to ensure proper and authorized use and dissemination."

In addition, Section VI.C. of the MOU states "The Providing Agency shall receive an annual affirmation from the Requesting Party indicating compliance with the requirements of this agreement no later than 45 days after the anniversary date of this agreement."

According to interviews with DAVE users, it does not appear that the Agency monitors usage on an "on-going basis. There is no documentation to support that the Agency has performed any type of monitoring of user accesses to DAVE.

The Agency also does not consistently submit annual affirmations. There were no annual affirmations, as required by the MOU, for 2009 or 2010. After a final reminder from DHSMV on May 10, 2011 that threatened a "disruption in service," Investigations sent an Annual Affirmation Statement to DHSMV on May 18, 2011. Investigations sent a timely Affirmation Statement for 2012.

Neither Investigations nor Support Services have a process or maintain documentation to ensure compliance with the MOU requirements for on-going monitoring, performing an annual audit and submitting an Annual Affirmation Statement. Failing to submit an Annual Affirmation Statement could have resulted in the Agency losing access to DAVE, which is a useful tool for both investigations and parking enforcement.

Recommendations

1. To meet the on-going monitoring requirement, the Staff Person should review and document users' accesses to DAVE on a quarterly basis.
2. The Staff Person should timely complete and document an annual audit and submit an Annual Affirmation Statement to DHSMV. The audit guide and Annual Affirmation Statements are located at: https://idave.flhsmv.gov/message_center.html

3. The Staff Person should incorporate all responsibilities addressed in this report, including performing the annual audit and quarterly monitoring, in written desk procedures.

Management Response

The appointed staff person within the Office of Inspector General who is independent of the DAVE process will develop a process and maintain documentation to ensure compliance with the MOU requirements for on-going monitoring, performing an annual audit, and submitting an Annual Affirmation Statement.

Finding 10: Secretary's Signature for Agreements

An Agency draft Policy/Procedure # 4028, although not yet approved as of this report's issue date, contains a provision that all Agency agreements, including MOUs, are to be approved and signed by the Secretary. Agency management appears to have been aware of the policy as evidenced by our review of Agency agreements signed by the Secretary or a Deputy Secretary from mid-2011 to 2012.

For both the 2008 and 2011 MOUs, the Chief of Investigations, who was also the DAVE Administrator, signed the agreement for the Agency.

Even though the Chief of Investigations might not have been aware that the Secretary should sign Agency agreements, he should have checked with senior management to confirm who was authorized to sign for the Agency. Because only the Chief of Investigations was aware of the MOU, the Agency was at greater risk of incurring liability because they were not ensuring users were being properly monitored. Also, the offending user would be liable for misuse. Recent newspaper articles reported Florida law enforcement officers misusing the Driving and Vehicle Information Database. Some officers have been disciplined or fired. One of the persons whose information was accessed improperly by law enforcement officers has filed a federal lawsuit against the officers and the agencies that employ the officers.

Recommendation

The Secretary should sign the DHSMV MOU.

Management Response

The Chief of Investigations appointed in 2013 is aware that the Agency head is required to execute such inter-agency agreements. All future memoranda of understanding will be reviewed and signed by the Agency head.

Finding 11: Ensuring Accountability

The MOU between DHSMV and the Agency only covers the use of DAVE. This MOU requires specific controls and monitoring by participating agencies.

One of Support Services' users does not always use DHSMV's DAVE system to perform his responsibility related to parking issues. He uses an older system (KDC) that is still being maintained by DHSMV. Although this system is not covered by the MOU, the data is still covered under Section 119.0712(2)(b), F.S. According to DHSMV, by July 2014, they will only support DAVID as an access tool for driver's license and tag information. Users of both KDC and DAVE will move to DAVID; however, their accesses will be limited to approved usage.

Because this user is accessing a system that appears to have no controls, the Agency would not be able to determine whether his accesses are appropriate and that he is complying with the statutory requirements related to driver license data when they are conducting either quarterly or annual reviews.

Recommendations

1. Investigations should request that DHSMV remove the Support Services user's access to KDC.
2. Any Agency user of DHSMV driver license data should be required to access only DAVE.

Management Responses

1. Investigations has received confirmation from DHSMV/Support Services that KDC access has been cancelled. The DAVE Administrator will keep the documentation supporting the cancellation on file.
   Support Services has contacted DHSMV's Technical Assistance Center to request the KDC access be cancelled.
2. Support Services has contacted DHSMV's Technical Assistance Center to request the KDC access be cancelled. Support Services staff is only accessing DAVE.

FINAL COMMENTS

Internal Audit would like to thank the management and staff of Investigations and Support Services for their assistance and cooperation extended to us during this engagement.

This page is left intentionally blank.

This page is left intentionally blank.

The Agency for Health Care Administration's mission is Better Health Care for All Floridians.
The Inspector General's Office conducts audits and reviews of Agency programs to assist the Secretary and other agency management and staff in fulfilling this mission.

This review was conducted pursuant to Section 20.055, Florida Statutes and in accordance with the *International Standards for the Professional Practice of Internal Auditing* as established by the Institute of Internal Auditors... The review was conducted by Karen Calhoun, CISA, CIGA, under the supervision of Mary Beth Sheffield, Audit Director, CPA, CIA, CFE, CIG. Please address inquiries regarding this report to the AHCA Audit Director by telephone at (850) 412-3978.

Copies of final reports may be viewed and downloaded via the internet at:
ahca.myflorida.com/Executive/Inspector_General/Internal_Audit/audit.shtml
Copies may also be obtained by telephone (850) 412-3990, by FAX (850) 487-4108, in person, or by mail at Agency for Health Care Administration, Fort Knox Center, 2727 Mahan Drive, Mail Stop #5, Tallahassee, FL 32308.