STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2018-071
December 2017

DEPARTMENT OF HEALTH

Licensing and Enforcement Information Database System (LEIDS)

Sherrill F. Norman, CPA
Auditor General

State Surgeon General and State Health Officer

The Department of Health is created by Section 20.43, Florida Statutes. The head of the Department is the State Surgeon General and State Health Officer who is appointed by the Governor subject to confirmation by the Senate. Dr. Celeste Philip served as the State Surgeon General and State Health Officer during the period of our audit.

The team leader was Earl M. Butler, CISA, CFE, and the audit was supervised by Tina Greene, CPA, CISA.

Please address inquiries regarding this report to Arthur Hart, CPA, Audit Manager, by e-mail at arthart@aud.state.fl.us or by telephone at (850) 412-2923.

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

FLAuditor.gov

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 HEALTH

Licensing and Enforcement Information Database System (LEIDS)

SUMMARY

This operational audit of the Department of Health (Department) focused on evaluating selected information technology (IT) controls applicable to the Licensing and Enforcement Information Database System (LEIDS) and included a follow-up on applicable findings noted in our report No. 2015-119. Our audit disclosed the following:

Finding 1: LEIDS application input edits for ensuring data accuracy and validity need improvement.

Finding 2: During the period July 2016 through July 2017, the Department had not established written procedures for, and had not performed, periodic reviews of LEIDS user access privileges.

Finding 3: The Department's access control procedures need improvement to better ensure that access privileges granted for LEIDS users are timely deactivated when users separate from employment.

Finding 4: Some LEIDS user access privileges did not always provide for individual accountability and were not limited to only what was necessary in the performance of the users' assigned job duties.

Finding 5: The Department did not maintain complete and accurate LEIDS access authorization documentation, thereby limiting management's assurance that LEIDS user access privileges were authorized and appropriately assigned.

Finding 6: Some Department configuration management controls need improvement to ensure that authorization, testing, and approval activities for LEIDS program and data changes are documented and that changes are moved into the production environment by appropriate personnel.

Finding 7: Certain Department security controls related to user authentication, logging and monitoring, and the protection of confidential and exempt data for LEIDS and related IT resources need improvement.

BACKGROUND

State law[1] requires the Department of Health (Department) to regulate health practitioners for the preservation of the health, safety, and welfare of the public. The Division of Medical Quality Assurance (Division) within the Department is responsible for licensing and regulating health care practitioners (e.g., medical doctors, nurses, and pharmacists) and certain health care facilities. Specifically, the Division plans, develops, coordinates, and manages health care professional regulatory boards and councils; reviews and investigates consumer complaints; and licenses health care professionals and a limited number of facilities and establishments (e.g., dental laboratories, electrolysis facilities, massage establishments, office surgery registrations, optical establishments, optometry branch offices, and pain management clinics).

[1] Section 20.43, Florida Statutes.

The Division's three key business processes are licensing, enforcement, and public information. The Division's:

- Licensing activities include, but are not limited to, preparing and administering licensure examinations; issuing and renewing licenses; tracking licensure conditions and restrictions; monitoring compliance with continuing education and financial responsibility requirements; and evaluating and approving training programs and continuing education providers.
- Enforcement activities include receiving, analyzing, and investigating complaints and reports; tracking licensees' compliance with disciplinary sanctions; inspecting health care facilities; issuing citations and emergency suspension and restriction orders; conducting disciplinary proceedings; and combating unlicensed activity.
- Public information and data activities include providing easy public access to licensing and disciplinary information; ensuring that data is accurate, timely, consistent, and reliable; and collecting and reporting workforce data.

In November 2014, the Division replaced the Computer Oriented Medical Practitioner Administration System (COMPAS) with the Licensing and Enforcement Information Database System (LEIDS), a new information technology (IT) solution to support the Division's key business processes.

FINDINGS AND RECOMMENDATIONS

Finding 1: Application Input Edits

Effective application input controls provide reasonable assurance that erroneous data is prevented or detected before processing and help ensure the accuracy and validity of data. As part of our audit we evaluated LEIDS input screens for pharmacy license applications, pharmacy facility inspections, and disciplinary actions and found that some application input edits need improvement. Specifically, we selected:

- The *Owner Information* screen to test whether the input edits adequately prevent the entry of erroneous data for pharmacy license applications. Our evaluation of the input edit controls as of June 8, 2017, disclosed that alphabetic characters were allowed in the telephone number, social security number, and zip code fields, and that a date was allowed in the date of birth field that would indicate that the owner was over 150 years old.
- The *Maintain Visit*, *Maintain Inspection*, and *Maintain Inspection Visits* screens to test whether the input edits adequately prevent the entry of erroneous data related to pharmacy facility inspections. Our evaluation of the input edit controls as of July 13, 2017, disclosed that:
    - On the *Maintain Visit* screen, dates were allowed in the start date and end date fields that would indicate an inspection of a pharmacy as early as the year 1850 and as late as the year 2050.
    - On the *Maintain Inspection* screen, dates were allowed in the start date and end date fields that would schedule an inspection of a pharmacy beginning in the year 2050 and ending in the year 9999.
    - A reinspection should be scheduled to occur 30 to 60 days after a failed initial inspection. The inspect after date should be set to 30 days after the initial inspection and the inspect before date should be set to 60 days after the initial inspection to ensure that the reinspection falls within the 30 to 60-day time frame. However, on the *Maintain Inspection Visits* screen, a date was allowed in the inspect before date field that preceded the date entered in the inspect after

date field for pharmacy inspections even though the inspect before date should always follow the inspect after date.

- The *Complaint* and *Respondent* screens to test whether the input edits adequately prevent the entry of erroneous data related to disciplinary actions. Our evaluation of the input edit controls as of July 21, 2017, disclosed that for the respondent screen, invalid data was allowed in the city, state, and zip code fields and alphabetic characters were allowed in the telephone number field for health care practitioners being investigated for disciplinary actions.

In response to our audit inquiry, Department management indicated that the lack of certain field edits was an oversight by the developer in the original design of the system and that system corrections will be initiated. The establishment of appropriate application input edits would help ensure the accuracy and validity of LEIDS data.

Recommendation: We recommend that Department management improve application input edits to ensure the accuracy and validity of LEIDS data.

Finding 2: Periodic Review of Access Privileges

Agency for State Technology (AST) rules[2] require agency control measures to address responsibilities of information stewards that facilitate periodic reviews of access rights with information owners. The frequency of the reviews must be based on system categorization or assessed risk. Periodic reviews of user access privileges help ensure that only authorized users have access and that the access provided to each user remains appropriate. An effective periodic access review consists of identifying the current access privileges of all users within the system, evaluating the access privileges necessary for the users' current job duties, and updating the authorization forms and the actual access privileges to reflect the appropriate access privileges.

As similarly noted in our report No. 2015-119 (finding No. 7), our audit procedures disclosed that, during the period July 2016 through July 2017, the Department had not established written procedures for, and had not performed periodic reviews of, LEIDS user access privileges. In response to our audit inquiry, Department management stated that, due to the risk that the Department may exceed the number of LEIDS software licenses purchased, Department staff conduct periodic access reviews to identify the user accounts that can be deactivated and the licenses reassigned to new user accounts. Department management also stated that they review the LEIDS roles annually to determine whether the roles should be modified based on business process changes. In addition, the Department deactivates accounts after 90 days of inactivity. However, these reviews do not include an evaluation of each user's access privileges granted to LEIDS.

The establishment of procedures for, and the performance of, periodic reviews of LEIDS user access privileges would increase management's assurance that the access privileges defined for LEIDS users are authorized and remain appropriate.

Recommendation: We recommend that Department management establish and implement procedures for the periodic review of LEIDS user access privileges to ensure that the access privileges are authorized and remain appropriate.

[2] AST Rule 74-2.003(1)(a)6., Florida Administrative Code.

Finding 3: Timely Deactivation of Access Privileges

AST rules[3] require each agency to manage identities and credentials for authorized devices and users and ensure IT access is removed when the IT resource is no longer required. Prompt action to deactivate access privileges when a user separates from employment or access to the information is no longer required is necessary to help prevent misuse of the access privileges.

As part of our audit procedures we selected 6 of the 30 Division employees who separated from Department employment during the period July 27, 2016, through April 13, 2017, to evaluate whether the former employees had active LEIDS access privileges as of May 9, 2017. Our audit procedures disclosed that 2 of the 6 selected former employees had active LEIDS user accounts as of May 9, 2017, although they had separated from Department employment on February 11, 2017, and April 13, 2017, respectively. Subsequent to our audit inquiry, the former employees' LEIDS user accounts were deactivated on August 11, 2017, or 181 days and 120 days after the employees' separation dates.

Additional audit procedures disclosed that, although the other 4 selected former employees' LEIDS user accounts were not active as of May 9, 2017, the accounts remained active from 8 to 104 days after the employees separated from Department employment. Table 1 shows the employment separation and account deactivation dates for each of these 4 former employees.

Table 1

Additional LEIDS User Accounts Untimely Deactivated

User Account	Employment Separation Date	Account Deactivation Date	Number of Days After Separation
1	August 3, 2016	August 11, 2016	8
2	November 18, 2016	December 16, 2016	28
3	December 17, 2016	March 31, 2017	104
4	January 27, 2017	March 6, 2017	38

Additionally, while evaluating whether service organization employees with LEIDS access privileges underwent appropriate background screenings, we noted that a service organization employee separated from the service organization in May 2014 but still had an active LEIDS user account as of May 9, 2017, approximately 1,075 days after the date of separation.

Contrary to AST rules,[4] Department policy[5] requires user accounts to be deleted within 30 days of employment separation, for nonuse of an account for 60 consecutive days, or upon notification of a security violation. In response to our audit inquiry, Department management stated that they will develop a script that will run daily to identify users with 60 days of inactivity to ensure compliance with Department policy and will modify the Department's contract with the service organization to include the vendor's responsibility to notify the Department within 30 days of a user's employment separation.

[3] AST Rule 74-2.003(1)(a)8., Florida Administrative Code.

[4] AST Rule 74-2.003(1)(a)8., Florida Administrative Code.

[5] Department of Health *Information Technology Information Security and Privacy Policy 10, Information Technology Security* (DOHP 50-10.10-16).

Allowing former Department or service organization employees' LEIDS user accounts to remain active 30 days or more beyond employees' separation dates, rather than promptly deactivating the user accounts when the access privileges are no longer needed (e.g., within 1 to 2 business days of an employee's separation from employment), increases the risk that the access privileges may be misused by a former Department or service organization employee or others to make changes to or inappropriately access confidential LEIDS data.

Recommendation: We recommend that Department management improve procedures to ensure that the LEIDS user accounts of former Department and service organization employees are more timely deactivated.

Finding 4: Appropriateness of Access Privileges

Effective access controls include measures that restrict user access privileges to only what is necessary in the performance of the user's assigned job duties, promote an appropriate separation of duties, and provide for individual accountability. Appropriately restricted access privileges help protect data and IT resources from unauthorized modification, loss, or disclosure.

Our audit procedures disclosed that some inappropriate and unnecessary access privileges existed in the production LEIDS application and Oracle database. Specifically:

- To evaluate the appropriateness of LEIDS application access privileges granted to Department users, we selected 40 of the 666 Department users with 676 active LEIDS user accounts as of May 9, 2017, and requested Department supervisors to verify the appropriateness of the access privileges granted. Our evaluation disclosed that 20 of the 40 selected users had access privileges that were determined by Department supervisors to be inappropriate and excessive. A similar finding was noted in our report No. 2015-119 (finding No. 7). In response to our audit inquiry, Department management indicated that the modification or removal of user access privileges is dependent upon the consistent submittal of appropriate documentation to the System Support Services Section by the user's supervisor when access privileges are no longer required.
- Additional audit procedures disclosed that 31 of the 720 active LEIDS user accounts[6] as of May 9, 2017, were generic or unassigned user accounts with various levels of access privileges and did not provide for individual accountability. Of the 31 generic or unassigned user accounts, 25 were initially intended to be used by the Department's service organization. In response to our audit inquiry, Department management indicated that 24 of these accounts were legacy accounts that should not have been transferred over during the conversion from COMPAS to LEIDS and 1 account had been assigned to a user but the name had been lost in the conversion. The remaining 6 accounts were Department accounts that were not assigned to specific users. A similar finding was noted in our report No. 2015-119 (finding No. 7).
- Our review of LEIDS database accounts disclosed that the database administrators (DBAs) had the ability to log on to the LEIDS database with three different schema[7] accounts that could update LEIDS objects. Specifically, we noted that, as of June 15, 2017, the DBAs shared the three schema accounts and corresponding passwords to manage certain database resources instead of using unique database accounts to provide for individual accountability. In response to our audit inquiry, Department management indicated that vendor involvement would be required to

[6] LEIDS user accounts consisted of 676 assigned and 6 generic or unassigned Department user accounts, and 13 assigned and 25 generic or unassigned service organization user accounts, for a total of 720 LEIDS user accounts.

[7] A schema is a collection of database objects (e.g., tables, views, and stored procedures) that are owned by a schema account. Schema accounts grant access to specific logical data structures owned by the accounts.

establish individual DBA accounts with access privileges to the database objects owned by the three schema accounts.

Inappropriate or unnecessary access to LEIDS IT resources and the lack of individual accountability when accessing LEIDS IT resources increase the risk of unauthorized modification, loss, or disclosure of LEIDS data and related IT resources.

Recommendation: The Department should implement effective access controls that limit LEIDS user access to only those access privileges that are necessary to perform the user's assigned job duties, promote an appropriate separation of duties, and provide for individual accountability.

Finding 5: Access Authorization Documentation

AST rules[8] require each agency to manage identities and credentials for authorized devices and users and establish control measures that address responsibilities of information stewards that include administering access to systems and data based on documented authorizations. Effective access authorization practices include, among other things, the use of access authorization forms to document the user access privileges authorized by management and to facilitate the complete and accurate assignment of user access privileges.

Department procedures[9] require users requesting access to LEIDS to submit a Licensing System Access Request form (access authorization form) to the System Support Services Section at least 5 business days prior to the access effective date. To evaluate whether LEIDS access privileges granted were authorized and appropriately assigned, we requested for examination access authorization forms for 40 of the 666 Department users with 676 active LEIDS user accounts as of May 9, 2017. Our examination disclosed that some access authorization forms could not be provided, did not include supervisor approval, or did not match the user access privileges granted and, as a result, Department records did not demonstrate that the LEIDS access privileges granted were authorized by management. Specifically, we found that:

- Department management did not provide access authorization forms for 9 of the 40 selected users.
- Access authorization forms for 3 of the remaining 31 selected users were missing supervisor approvals.
- The access privileges noted on the 31 access authorization forms provided did not match the actual LEIDS user access privileges granted.

The maintenance of access authorization records enhances management's ability to ensure and demonstrate that access privileges granted for users are appropriate for the users' assigned job duties. A similar finding was noted in our report No. 2015-119 (finding No. 7).

Recommendation: We recommend that Department management improve controls to ensure that access privileges are only granted pursuant to appropriately completed and approved access authorization forms and require that such forms be retained.

[8] AST Rule 74-2.003(1)(a)6., Florida Administrative Code.

[9] Department of Health *Division of Medical Quality Assurance User Access to MQA Licensing Database* (DOHP 385-SSS02-15).

Finding 6: Change Management Controls

Effective change management controls are intended to ensure that all program modifications are properly authorized, tested, and approved for implementation into the production environment and all data changes are appropriately authorized, approved, and implemented into the production database. Additionally, effective change management controls ensure that a group independent of the user and the programmers control movement of programs and data among libraries. The effectiveness of ensuring that only approved program and data changes are implemented is enhanced when program and data changes that have been moved into the production environment are reviewed for appropriateness.

As part of our audit procedures, we selected the seven program changes and the four data changes made to LEIDS during the period July 1, 2016, through May 26, 2017, to evaluate the adequacy of the program and data change management controls. For program changes, the Division is responsible for authorizing, testing, and approving program changes for implementation and the vendor is responsible for programming and implementing the program changes into the production environment. For data changes, the Division is responsible for authorizing and approving for implementation and the Office of Information Technology (OIT) is responsible for implementing the data changes into the production database.

Our audit disclosed that the LEIDS program and data change management controls need improvement. Specifically, we found that Department records did not evidence that the seven program changes were appropriately authorized or tested by the Division before being sent to the vendor, or appropriately approved by the Division to be moved into the production environment. Also, two of the four data changes were moved into the production environment by the programmer who made the data change.

The absence of appropriate program and data change controls increases the risk that program and data changes may not be implemented in a manner consistent with management's expectations.

Recommendation: The Department should improve LEIDS application program and data change management procedures to ensure that all program and data changes moved into the production environment are properly authorized, tested, and approved. We also recommend that the Department ensure that data changes are not moved into the production environment by the programmer who made the change.

Finding 7: Security Controls – User Authentication, Logging and Monitoring, and Protection of Confidential and Exempt Data

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain security controls related to user authentication, logging and monitoring, and the protection of confidential and exempt data need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising LEIDS data and related IT resources. However, we have notified appropriate Department management of the specific issues.

The lack of appropriate LEIDS security controls related to user authentication, logging and monitoring, and the protection of confidential and exempt data increases the risk that the confidentiality, integrity, and availability of LEIDS data and related IT resources may be compromised.

Recommendation: To ensure the confidentiality, integrity, and availability of LEIDS data and related IT resources, we recommend that Department management improve certain LEIDS security controls related to user authentication, logging and monitoring, and the protection of confidential and exempt data.

PRIOR AUDIT FOLLOW-UP

Except as discussed in Findings 2, 4, and 5, the Department had taken corrective actions for the applicable findings included in our report No. 2015-119.

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 IT operational audit from April 2017 through July 2017 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 the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected business process application controls over transaction data input, processing, output, and interfaces applicable to LEIDS during the period July 2016 through July 2017. The audit also included selected application-level general controls over logical access and change management related to LEIDS. The overall objectives of the audit were:

- To determine the effectiveness of selected information technology (IT) controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.
- To determine whether management has corrected, or is in the process of correcting, deficiencies disclosed in finding Nos. 5, 6, and 7 of our report No. 2015-119.
- 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 the IT system and controls 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 IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT system and controls included within the scope of this 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 the audit; obtaining an understanding of the IT system and controls; 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 the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items 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 contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting this audit, we:

- Interviewed Department personnel and reviewed documentation to obtain an understanding of LEIDS, including the:
    - Application background information for LEIDS, such as the purpose or goals involving financial, operations, and compliance requirements.
    - Data and business process flows for LEIDS, including interface processing. We also identified and documented key sources of data input, key application transactions and processes, key types of application data output, and key interfaces related to LEIDS.
    - IT computing platform for the LEIDS application including identification of the applicable hardware and software such as servers, operating systems, and security software related to the application.
- Evaluated LEIDS transaction data input controls related to health care practitioner and health care facility licenses, health care practitioner disciplinary actions, and health care facility inspections. Specifically, we:
    - Examined the online LEIDS screens to evaluate whether the Department implemented data encryption for the manually input data in screen fields and file uploads to control and limit access to confidential data and prevent unauthorized access during transmission.
    - Examined Department procedures and LEIDS screens such as the *Desktop Transaction Checklist Processing Procedures,* the *Pharmacy Intern US Graduate Licensure by Examination for U.S. Graduates* procedure, the *Checklist and Approval Screens for Pharmacist Applicants*, and the *Checklist and Approval Screens for Pharmacy Facility Applicants* to evaluate the adequacy of guidance regarding the review of data input checklists in correcting invalid data entry.
    - Evaluated the adequacy of LEIDS input edit controls as of June 2, 2017, in preventing the entry of erroneous pharmacist application data. Specifically, we examined the online field edits on the *Pharmacist License Application by Exam – Name and Personal Details* screen to evaluate whether the data input edits prevented the entry of erroneous data in the social security and visa number fields.
    - Evaluated the adequacy of LEIDS input edit controls as of June 8, 2017, in preventing the entry of erroneous pharmacy application data. Specifically, we examined the online field edits on the *Pharmacy License Application – Owner Information* screen to evaluate whether the

data input edits prevented the entry of erroneous data in the telephone number, social security number, date of birth, state, and zip code fields.

- Evaluated the adequacy of LEIDS input edit controls as of July 13, 2017, in preventing the entry of erroneous pharmacy facility inspection data. Specifically, we examined the online field edits on the *Pharmacy Facility Inspection* screens (i.e., *Maintain Visits, Maintain Inspections, Maintain Inspection Visits*) to evaluate whether the data input edits prevented the entry of erroneous data in various fields.
- Evaluated the adequacy of LEIDS input edit controls as of July 21, 2017, in preventing the entry of erroneous disciplinary action data. Specifically, we examined the online field edits on the *Disciplinary Action – Complaint* and *Respondent* screens to evaluate whether the data input edits prevented the entry of erroneous data in various fields.
- Inspected the *Auditing CNA Files* procedure to evaluate whether a control was in place for follow up on deficiency letters.
- Inspected the *Investigative Service Unit Conduct Inspections Desk Guide* and the *Open Inspections Workload For Profession 2205: Pharmacy* report to evaluate whether a control was in place to ensure that the appropriate number and percentage of routine inspections are assigned to an inspector.
- Inspected the *ISU Employee Performance Errors – Inspections Missing Visit After Dates* report to evaluate whether a control was in place to ensure that "Visit After" dates are in place for pharmacies that are new or have a change of location or ownership.
- Inspected the *Closed Inspections Workload For Profession 2205: Pharmacy* report to evaluate whether a control was in place to detect whether any pharmacy facility inspections were performed after the "Inspect Before" dates and to ensure that logical inspection start and end dates are entered by the inspector.
- Inspected various reports such as the *M310 Qualified Applicant Data Errors 8022: Board of Pharmacy* report, the *Open Application* report, the *Review Vital Statistics Matches Profession 2201: Pharmacist* report, the *All Initial Application Processing 2201: Pharmacist report,* and the *Unassigned Cash* report to evaluate whether a control was in place to detect errors in the data previously input by pharmacist or pharmacy facility applicants or from current licensee status changes.
- Inspected various reports such as the *CSU Actv Error Report - Missing Case Status 30 or 35* and the *CSU Status 10 Transfers Without 456 Activity Entry Summary* reports to evaluate whether a control was in place to identify missing activity codes that should be associated with certain active disciplinary investigations.
- Inspected the *DOH99 Reconcile* report and the *GRAILS AuditLog List* to evaluate whether a control was in place to detect file uploading and communication errors.

- Evaluated LEIDS transaction data processing controls related to health care practitioner and health care facility licenses, health care practitioner disciplinary actions, and health care facility inspections. Specifically, we:
  - Inspected the *BOA Manual Receipting Instructions* procedure and documented our understanding of online credit card payment processes and the procedures for making corrections for certain receipts (such as duplicate credit card transactions).
  - Inspected the *Consumer Services Unit Duplicate Complaints Desk Guide* to evaluate whether a control was in place to prevent the creation of duplicate investigations arising from multiple sources of complaints received on the same respondent (health practitioner).

- Examined the LEIDS history logs for pharmacy and pharmacist applications to evaluate whether the system adequately captured updates to checklist items and application statuses and identifies when the updates occurred and by whom.
- Examined the LEIDS history logs for pharmacy inspections to evaluate whether the system adequately captured updates to certain inspection screens and identifies when the updates occurred and by whom.
- Examined the LEIDS history logs for enforcement activities to evaluate whether the system adequately captured updates to certain enforcement screens and identifies when the updates occurred and by whom.

- Evaluated LEIDS transaction data output controls related to the Division's reporting of health care practitioner and health care facility licenses, health care practitioner disciplinary actions, and health care facility inspections on the Department Web site. Specifically, we:
  - Examined various procedures related to annual and quarterly reports to evaluate whether the procedures were adequate to reasonably assure the integrity of the data in the reports published on the Department's Web site that contain statistical information on Department activities such as licensure, inspections, and enforcement.
  - Examined the *Quarterly and Annual Report Data Review Schedule and Source* procedures, an example *Annual Report (DXT700)*, and an example data approval e-mail to evaluate whether the procedures provided for an adequate review of the data reported on the final quarterly and annual reports.
  - Inspected the *Operational Support Service Unit Deputy Agency Clerk Manual* and other related documents to evaluate whether there were procedures in place for processing Board orders that implement disciplinary actions affecting a health care practitioner and for posting Board actions on the Department's Web site.
  - Reviewed the *Cash Management System*, *MQA Service Reporting System*, and *Treasury Receipt Processing* screens to evaluate whether information was available to aid in the reconciliation process to compare extracted payment information from LEIDS with deposit information in the Florida Accounting Information Resource Subsystem (FLAIR).
  - Inspected the *AHCA Clearing House* report for evidence that criminal history reporting errors were identified and resolved.
- Evaluated interface processing procedures between LEIDS and external systems, including reconciliation controls between LEIDS and FLAIR. Specifically, we:
  - Reviewed the Department's automated reconciliation procedures between the prior day payments on the database and the prior day bank settlement file.
  - Reviewed the Department's automated reconciliation procedures between the receipt batches for a work day and the settled database batches.
  - Reviewed the Department's automated notification processes indicating whether bank settlement files were successfully downloaded, reconciliation processes were successfully executed, and balancing issues were found.
  - Reviewed the *Batch Error Report* to evaluate the adequacy of error reporting for files uploaded to FLAIR.
- Evaluated the LEIDS user access controls related to user authorization and appropriateness. Specifically, we:
  - Reviewed the *User Access to MQA Licensing Database* policy and procedure to gain an understanding of the Department's requirements for requesting access to LEIDS.

- For 40 of the 666 Department users with 676 active LEIDS user accounts as of May 9, 2017, evaluated whether the access granted was documented, authorized, and appropriately assigned.
- Evaluated user access listings to evaluate whether generic or unassigned LEIDS user accounts existed.
- Reviewed the Department's service organization contract to gain an understanding of the requirements for level 2 background checks.
- Examined documentation for 6 of the 13 service organization employees with active LEIDS user accounts as of May 9, 2017, to evaluate whether level 2 background screenings were appropriately conducted and documented for the service organization employees.
- Reviewed the *Information Security and Privacy Policy 2* and the *User Access to MQA Licensing Database* policy and procedure to evaluate whether documented procedures for conducting periodic reviews of LEIDS user access privileges were in place.
- Determined whether the LEIDS access privileges for 6 former Division employees, selected from the 30 Division employees who separated from Department employment during the period July 27, 2016, through April 13, 2017, were active as of May 9, 2017.

- Evaluated the LEIDS technical access controls (e.g., directory services, operating system, database) related to the restriction of access privileges to individuals or processes having a valid business purpose and related to monitoring the use of the access privileges. Specifically, we:
  - Reviewed three LEIDS schema accounts to evaluate whether the accounts were shared and used as database log-on accounts.
  - Evaluated the effectiveness of logging and monitoring controls related to LEIDS IT resources.
  - Evaluated access controls designed to protect sensitive system resources.
  - Evaluated the effectiveness of logging and monitoring controls related to LEIDS IT resources.
- Reviewed the Department's *Information Security and Privacy Policy* and evaluated the adequacy of the LEIDS and database identification and authentication parameters identified on the LEIDS and database security policy screens.
- Evaluated the change management controls over LEIDS program and data changes. Specifically, we:
  - Reviewed the *MQA Change Management Plan* to evaluate whether the Department maintained current change management control procedures for LEIDS.
  - Examined the seven program changes for LEIDS completed during the period July 1, 2016, through May 11, 2017, to evaluate whether LEIDS program changes were appropriately authorized, tested, and approved for production.
  - Examined the four data changes for LEIDS completed during the period July 1, 2016, through May 26, 2017, to evaluate whether LEIDS data changes were appropriately authorized, approved, and moved into the production environment.
  - Reviewed server listings of the development, sandbox, configuration, test, and production environments to evaluate whether the environments were adequately separated.
  - Evaluated Department procedures for controlling access to LEIDS production code.
- 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, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE

Mission:
To protect, promote & improve the health of all people in Florida through integrated state, county & community efforts.

Florida HEALTH

Vision: To be the **Healthiest State** in the Nation

Rick Scott
Governor

Celeste Philip, MD, MPH
Surgeon General and Secretary

December 15, 2017

Ms. Sherrill F. Norman, CPA
Auditor General
Suite G74, Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Ms. Norman:

We are pleased to respond to the preliminary and tentative findings and recommendations made during the Office of the Auditor General's information technology operational audit of the Licensing and Enforcement Information Database System (LEIDS). Our response, as required by Section 11.45(4)(d), *Florida Statutes*, is enclosed.

We appreciate the efforts of you and your staff in assisting to improve our operations. Please contact Michael J. Bennett, CIA, CGAP, CIG, Inspector General, at (850) 245-4141, should you have any questions regarding our response.

Sincerely,

Celeste Philip, MD, MPH
Surgeon General and Secretary

CP/akm
Enclosure

cc: Michele Tallent, Deputy Secretary for Operations
Lucy C. Gee, MS, Director, Division of Medical Quality Assurance
Michael J. Bennett, CIA, CGAP, CIG, Inspector General
Tony K. Powell, Chief Information Officer, Office of Information Technology

Florida Department of Health
Office of the State Surgeon General
4052 Bald Cypress Way, Bin A-00 • Tallahassee, FL 32399-1701
PHONE: 850/245-4210 • FAX: 850/922-9453
FloridaHealth.gov

Preliminary and Tentative Findings

Report Number: To be determined
Report Title: *Licensing and Enforcement Information Database System*
Report Date: To be determined

No.	Finding	Recommendation	Management Response	Corrective Action Plan
1	Licensing and Enforcement Information Database System (LEIDS) application input edits for ensuring data accuracy and validity need improvement.	Department of Health (Department) management should improve application input edits to ensure the accuracy and validity of LEIDS data.	We concur.	**In progress.** The Division of Medical Quality Assurance's (MQA) vendor will correct the application input edits on the *Owner Information, Maintain Visit, Maintain Inspection, Maintain Inspection Visits*, and *Complaint and Respondent* screens. Changes unique to MQA will require custom development by the vendor. Projected Completion Date – June 29, 2018
2	During the period, July 2016 through July 2017, the Department had not established written procedures for, and had not performed, periodic reviews of LEIDS user access privileges.	Department management should establish and implement procedures for the periodic review of LEIDS user access privileges to ensure that the access privileges are authorized and remain appropriate.	We concur.	**In progress.** MQA will establish and implement written procedures for conducting periodic reviews of LEIDS user access privileges to ensure access privileges are authorized and appropriate to the user's position description. Additionally, MQA will conduct a review of all active LEIDS user accounts prior to implementing new periodic review procedures. Projected Completion Date – January 31, 2018
3	The Department's access control procedures need improvement to better ensure that access privileges granted for LEIDS users are timely deactivated when users separate from employment.	Department management should improve procedures to ensure that the LEIDS user accounts of former Department and service organization employees are more timely deactivated.	We concur.	**In progress.** MQA will establish and implement procedures to ensure LEIDS user accounts are timely deactivated when users separate from employment. Additionally, MQA will conduct a review of all active LEIDS user accounts to ensure all users are current employees. Additionally, MQA will explore connecting LEIDS to a Department single sign-on protocol for authentication in the future, allowing deactivation through normal Bureau of Personnel and Human Resource Management separation processing. Projected Completion Date – January 31, 2018

No.	Finding	Recommendation	Management Response	Corrective Action Plan
4	Some LEIDS user access privileges did not always provide for individual accountability and were not limited to only what was necessary in the performance of the users' assigned job duties.	Department management should implement effective access controls that limit LEIDS user access to only those access privileges that are necessary to perform the user's assigned job duties, promote an appropriate separation of duties, and provide for individual accountability.	We concur.	**In progress.** MQA will establish review procedures to ensure user access controls to LEIDS are specific to job duties. This will include establishing new procedures for granting temporary access to users who are assigned temporary responsibilities based on the needs of the organization. Additionally, MQA will conduct a review of all active LEIDS user accounts to ensure access privileges are limited to only what is necessary in the performance of the users' assigned job duties. The Department will work with its vendor to establish and implement a means whereby all database administrators (DBAs) access and administrative changes can be attributed to a single DBA. Projected Completion Date – January 31, 2018
5	The Department did not maintain complete and accurate LEIDS access authorization documentation, thereby limiting management's assurance that LEIDS user access privileges were authorized and appropriately assigned.	Department management should improve controls to ensure that access privileges are only granted pursuant to appropriately completed and approved access authorization forms and require that such forms be retained.	We concur.	**In progress.** MQA will review existing procedures to ensure user access controls to LEIDS are specific to job duties and only granted when the appropriate form is received by the System Support Services staff and authorized by management. This will include establishing procedures for granting temporary access to users who are assigned temporary responsibilities based on the needs of the organization. Additionally, MQA will conduct a review of all active LEIDS user accounts to ensure LEIDS user access privileges are limited to what the user needs to perform assigned job duties and to verify appropriate authorization form was received and retained. Projected Completion Date – January 31, 2018
6	Some Department configuration management controls need improvement to ensure that authorization, testing, and approval activities for LEIDS program and data changes are documented and that changes are moved into the production environment by appropriate personnel.	(6.1) Department management should improve LEIDS application program and data change management procedures to ensure that all program and data changes moved into the production environment are properly authorized, tested, and approved.	We concur.	(6.1) **In progress.** MQA and the Information Technology(IT)/MQA Application Development Section will evaluate existing Change Management Procedures and develop a user guide to ensure any program or data changes moved into the production environment are properly authorized, tested, and approved by the appropriate business owner and proper documentation is retained. This will include training appropriate staff on the change management procedures. Projected Completion Date – January 31, 2018
		(6.2) Department management should ensure that data changes are not moved into the production environment by the programmer who made the change.	We concur.	(6.2) **In progress.** The IT/MQA Application Development Section will establish and implement written procedures to ensure data changes are not moved into the production environment by the programmer who made the change. Projected Completion Date – December 15, 2017

Preliminary and Tentative Findings - *Licensing and Enforcement Information Database System (LEIDS)*

No.	Finding	Recommendation	Management Response	Corrective Action Plan
7	Certain Department security controls related to user authentication, logging and monitoring, and the protection of confidential and exempt data for LEIDS and related IT resources need improvement.	To ensure the confidentiality, integrity, and availability of LEIDS data and related IT resources, Department management should improve certain LEIDS security controls related to user authentication, logging and monitoring, and the protection of confidential and exempt data.	We concur.	**In progress.** DOH concurs with user authentication, logging, and monitoring findings. MQA will improve certain LEIDS security controls related to user authentication, logging and monitoring, and the protection of confidential and exempt data. Projected Completion Date – June 29, 2018