STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2017-051
November 2016

DEPARTMENT OF HEALTH

Acquired Immune Deficiency Syndrome Information Management System

Sherrill F. Norman, CPA
Auditor General

State Surgeon General of the Department of Health

Section 20.43, Florida Statutes, creates the Department of Health. The head of the Department is the State Surgeon General of the Department of Health who is appointed by the Governor, subject to confirmation by the Senate. During the period of our audit, the following individuals served as State Surgeon General.

Celeste Philip, MD	From May 18, 2016
	Interim from March 11 to May 17, 2016
John H. Armstrong, MD	To March 10, 2016

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:

http://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 HEALTH

Acquired Immune Deficiency Syndrome Information Management System

SUMMARY

This operational audit of the Department of Health (Department) focused on evaluating selected information technology (IT) controls applicable to the Acquired Immune Deficiency Syndrome Information Management System (AIMS2.0). Our audit disclosed the following:

Finding 1: The Department had not established policies and procedures for various AIMS2.0 processes or user responsibilities, increasing the risk that tasks related to various AIMS2.0 processes and user responsibilities will not be carried out consistently and in a manner pursuant to management's expectations.

Finding 2: The Department had not created application design documentation for AIMS2.0 to ensure that AIMS2.0 aligned with management's business requirements.

Finding 3: The Department had not established procedures for the periodic review of AIMS2.0 user access privileges and did not perform periodic reviews of access privileges.

Finding 4: Documentation supporting authorization of access privileges for AIMS2.0 for some employees was missing or incomplete or did not match the user access privileges granted. In addition, the Department's local office for AIMS2.0 had not established written procedures for the security administration of AIMS2.0.

Finding 5: The access privileges of some AIMS2.0 users did not restrict users to only those functions appropriate and necessary for their assigned job duties.

Finding 6: The Department did not timely deactivate the AIMS2.0 accounts for some former employees to prevent the former employees or others from misusing the former employees' access privileges.

Finding 7: The Department had not implemented a complete system development life cycle methodology to ensure that security or functionality requirements were included throughout the development and maintenance of AIMS2.0.

Finding 8: The Department had not established controls to ensure that all program changes related to AIMS2.0 that had been implemented into the production environment were appropriately authorized, tested, and approved.

Finding 9: Certain security controls related to user authentication, access privileges, and monitoring for AIMS2.0 and related IT resources need improvement to ensure the confidentiality, integrity, and availability of AIMS2.0 data and related IT resources.

BACKGROUND

The Department of Health (Department) was established by State law.[1] On April 1, 2013, the Department implemented a new contract management and reporting system for the Human Immunodeficiency Virus/Acquired Immune Deficiency Syndrome (HIV/AIDS) section called the Acquired Immune Deficiency Syndrome Information Management System (AIMS2.0). AIMS2.0 was developed to manage, monitor, and track funds received from various sources for the care of the HIV/AIDS population throughout the State of Florida. The primary information technology (IT) infrastructure for AIMS2.0 is located in Tallahassee, Florida.

FINDINGS AND RECOMMENDATIONS

Finding 1: Policies and Procedures

Effective management practices include the establishment of policies and procedures that describe management's expectation for controlling Department operations. Written policies and procedures and other documentation, such as training materials and user manuals, help ensure that management directives are clearly communicated, understood, and followed by staff.

Our review of AIMS2.0 documentation revealed that no policies and procedures had been established to outline the various AIMS2.0 processes or user responsibilities. In response to our audit inquiry, Department management stated that they are currently in the process of developing written policies and procedures and have issued a draft user manual.

Without written policies and procedures, the risk is increased that tasks related to AIMS2.0 processes and user responsibilities will not be carried out consistently and in a manner pursuant to management's expectations.

Recommendation: We recommend that Department management continue efforts to establish policies and procedures for AIMS2.0 processes and user responsibilities.

Finding 2: Application Design Documentation

Application design documentation provides the basis for validating that the processing design of the business application meets management's requirements and includes controls to ensure the confidentiality, availability, and integrity of the IT resources and data. Continued maintenance of application design documentation helps management ensure that changes to the original application design continue to align with management's business requirements.

Our audit procedures disclosed that the Department had not created detailed application design documentation for AIMS2.0 (e.g., a comprehensive business requirements document containing system edits). In response to our audit inquiry, Department contract staff stated that, due to competing priorities and a lack of time and resources, comprehensive business requirement documents were not available.

[1] Section 20.43, Florida Statutes.

Detailed design documentation that represents the current state of AIMS2.0 business processes would provide increased assurance that AIMS2.0 aligns with management's business requirements.

Recommendation: To help ensure that AIMS2.0 aligns with Department management's business requirements, we recommend that Department management create and maintain application design documentation.

Finding 3: Periodic Reviews of User Access Privileges

Agency for Enterprise Information Technology (AEIT) rules[2] required agency information owners to review access rights (privileges) periodically based on risk, access account change activity, and error rate. Periodic reviews of user access privileges help ensure that only authorized users have access and that the access provided to each user remains appropriate.

Our audit procedures disclosed that Department management had not established procedures for the periodic review of AIMS2.0 user access privileges and did not perform periodic reviews of AIMS2.0 user access privileges during the period July 2015 through June 2016. In response to our audit inquiry, Department management indicated that the lack of procedures requiring periodic review of AIMS2.0 user access privileges was due to an oversight.

Without periodic reviews of AIMS2.0 user access privileges, management has limited assurance that user access privileges are authorized and appropriate.

Recommendation: We recommend that Department management establish procedures requiring that the authorization and appropriateness of AIMS2.0 user access privileges be periodically reviewed and ensure that such reviews are timely performed.

Finding 4: Documentation of User Access Authorizations

Effective access authorization practices include, among other things, the use of access authorization forms to document the user access privileges authorized by management. Access authorization documentation should be maintained in an appropriate manner to facilitate the complete and accurate assignment of user access privileges. Department Policy[3] required each Department program office to have written local information security and privacy procedures, such as security administration procedures, to ensure the security of information and protect the confidentiality, data integrity, and access to information. However, we noted that the AIMS2.0 program office did not have documented procedures to be used for the security administration of AIMS2.0.

We requested access authorization documentation for 14 of the 138 users with update and view access privileges to AIMS2.0 as of June 13, 2016, to determine whether the access privileges granted for

[2] AEIT Rule 71A-1.007(2), 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. On June 5, 2016, Chapters 71A-1 and 71A-2, Florida Administrative Code, were repealed. The AST adopted Rules 74-2.001 through 74-2.006, Florida Administrative Code, effective March 16, 2016, establishing the Florida Cybersecurity Standards. AST Rule 74-2.003(1)(a)6. requires that each agency shall facilitate periodic review of access rights with information owners. The frequency of the reviews shall be based on system categorization or assessed risk.

[3] Department of Health Information Security and Privacy Policy 50-10.1-16.

AIMS2.0 were appropriately authorized and documented. Our audit procedures disclosed that some access authorization forms were missing or not signed by the appropriate supervisor or did not match the user access privileges granted. Specifically:

- AIMS2.0 access authorization forms for 6 employees were missing and could not be provided by the Department.
- AIMS2.0 access authorization forms for 4 users were not signed by the appropriate supervisor.
- AIMS2.0 access authorization forms for 2 employees did not include appropriate access role information.
- The AIMS2.0 access role information authorized on the user access authorization form for 1 user did not match the user access privileges granted.

Documented security administration procedures help ensure that user access privileges are commensurate with management's direction. Additionally, the maintenance of appropriately authorized, complete, and accurate access authorization forms enhance management's ability to both ensure and demonstrate that user access privileges granted for users are appropriate for the users' assigned job duties.

Recommendation: We recommend that Department management improve controls to ensure that applicable security administration procedures are documented and that access authorization forms are retained, complete, and commensurate with management's direction.

Finding 5: Appropriateness of User Access Privileges

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

Our review of access privileges for 14 of the 138 AIMS2.0 active users as of June 13, 2016, disclosed that 3 users were granted update access privileges to AIMS2.0 that were inappropriate and unnecessary for the users' assigned job duties. According to Department management, the users' access privileges were deactivated on July 27, 2016, subsequent to our audit inquiry.

Efforts to ensure that users are granted only those access privileges that are appropriate and necessary for the users' assigned job duties would help protect AIMS2.0 data and related IT resources from unauthorized modification, loss, or disclosure.

Recommendation: We recommend that Department management limit user access privileges to AIMS2.0 data and IT resources to promote an appropriate separation of duties and restrict users to only those functions necessary for their assigned job duties.

Finding 6: Employee Access Deactivation

AEIT rules[4] require access authorization to be promptly removed when the user's employment is terminated or access to information resources is no longer required. Prompt action is necessary to ensure that the former employees or others do not misuse the former employees' access privileges.

Our review of the 138 active users as of June 13, 2016, disclosed 9 AIMS2.0 accounts for employees who separated from the Department during the period July 5, 2013, through March 2, 2016. As of June 13, 2016, the 9 former employees' AIMS2.0 accounts remained active for time periods ranging from 103 to 1,074 days after the employees separated from Department employment. Although the AIMS2.0 accounts were not timely deactivated, we noted that the former employees' AIMS2.0 accounts were not used subsequent to the employees' respective employment separation dates.

In response to audit inquiry, Department staff stated that, because they did not review the appropriateness of AIMS2.0 user access privileges (as noted in Finding 3), they had overlooked the necessity to remove user access at the time of employee separation. Without the timely deactivation of former employees' AIMS2.0 accounts, the risk is increased that the accounts may be misused by the former employees or others.

Recommendation: We recommend that Department management ensure that the AIMS2.0 accounts of former employees are timely deactivated.

Finding 7: System Development Life Cycle

An effective entitywide system development life cycle (SDLC) methodology details the procedures that are to be followed when systems and applications are being designed and developed, as well as when they are subsequently modified. The SDLC should provide a structured approach for identifying and documenting design, development, testing, implementation, and maintenance of systems and applications to meet the security and functional requirements of the entity.

Our audit tests disclosed that, while the Department had implemented a development release cycle process for the movement of program code into the production environment, a complete system development life cycle methodology was not documented to ensure that AIMS2.0 was developed and maintained in accordance with a structured approach to meet the program areas' security and functional needs.

Without a documented SDLC methodology, the risk is increased that necessary security or functional requirements may not be included in a system's development and maintenance.

Recommendation: We recommend that Department management establish a documented SDLC methodology to ensure that security and functional requirements are included in the maintenance of AIMS2.0.

[4] AEIT Rule 71A-1.007(6), Florida Administrative Code. AST Rule 74-2.003(1)(a)8., requires that IT access be removed when the IT resource is no longer required.

Finding 8: Change Management Controls

Effective change management controls over program changes ensure that only authorized, tested, and approved program changes are implemented into the production environment. Further, the effectiveness of change management controls is enhanced through controls that ensure that the change management control process is followed when program changes are implemented into the production environment.

Our audit procedures disclosed that Department change management controls need improvement. Specifically, we found that:

- Although the Department used a change management system for tracking the authorization, testing, approval, and implementation of program changes, the Department had not established controls, such as the use of a reconciliation process, to ensure that all program changes implemented into the production environment followed the Department's change management process.
- Eight of the 83 program changes related to AIMS2.0 and implemented during the period July 1, 2015, through May 20, 2016, were not appropriately authorized, and 4 of the 8 program changes were also not appropriately tested.

Absent effective change management controls to ensure that all program changes are authorized, tested, and approved, erroneous or unauthorized program changes may be implemented into the production environment without timely detection.

Recommendation: We recommend that Department management establish controls to ensure that only authorized, tested, and approved program changes related to AIMS2.0 are implemented into the production environment.

Finding 9: Security Controls – User Authentication, Access Privileges, and Monitoring

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, access privileges, and monitoring for AIMS2.0 and related IT resources need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising AIMS2.0 data and IT resources. However, we have notified appropriate Department management of the specific issues.

Appropriate security controls related to user authentication, access privileges, and monitoring for AIMS2.0 and related IT resources would help ensure the confidentiality, integrity, and availability of AIMS2.0 data and related IT resources.

Recommendation: We recommend that Department management improve certain security controls related to user authentication, access privileges, and monitoring for AIMS2.0 and related IT resources to ensure the confidentiality, integrity, and availability of AIMS2.0 data and related IT resources.

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 May 2016 through June 2016 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 IT controls applicable to AIMS2.0 during the period July 2015 through June 2016, and selected actions subsequent thereto. The audit included selected business process application controls over transaction data input, processing and output, and selected application-level general controls over logical access to programs and data, configuration management, and contingency planning. The overall objectives of the audit were:

- To determine the effectiveness of selected 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; the safeguarding of IT resources; and the effectiveness and efficiency of IT operations.
- 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 systems 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 systems 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 systems 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 AIMS2.0-related documentation to obtain an understanding of:
  - The AIMS2.0 background, including the AIMS2.0 purpose and goals involving financial, operations, and compliance requirements.
  - The AIMS2.0 computing platform including applicable hardware, operating system, database management system, and security software.
  - The AIMS2.0 data and business process flows, including key sources of data input related to the application.
  - The establishment of policies and procedures for AIMS2.0 processes and user responsibilities.
  - User account management processes for authorizing, creating, modifying, and revoking access to AIMS2.0.
  - Change management processes applicable to AIMS2.0, including identification of policies and procedures for change control.
- Evaluated the effectiveness of selected AIMS2.0 business process application controls related to data input. Specifically, we reviewed the eight online edits built into AIMS2.0 as of June 14, 2016, related to the entering of a new contract and monthly contract-related expenses to determine whether the edits were in place and operating effectively.
- Evaluated AIMS2.0 contingency planning controls for the prevention and minimization of damage and interruption in the event of a disaster, the development and documentation of a continuity of operations plan (COOP), and the periodic testing of the COOP.
- Evaluated Department procedures in place for the review of the appropriateness of AIMS2.0 access privileges.
- Evaluated access privileges granted for 14 of the 138 AIMS2.0 active users as of June 13, 2016, to determine whether the access granted was documented, authorized, and appropriate and evaluated an additional 8 user accounts for appropriateness of termination procedures.
- Evaluated administrative access privileges granted for the 8 applicable active users as of June 13, 2016, to determine the appropriateness of the access granted.
- Evaluated access privileges granted to the AIMS2.0 database for the 7 applicable active users as of June 27, 2016, to determine the appropriateness of the access granted.
- Evaluated user authentication controls related to AIMS2.0 and the AIMS2.0 database.
- Determined whether logging and monitoring for AIMS2.0 and related IT resources was performed.
- Evaluated the effectiveness of AIMS2.0 change management controls related to the authorization, testing, approval, and implementation of program changes into the production environment. Specifically, we evaluated 8 of the 83 program changes that were implemented into the production environment during the period July 1, 2015, through May 20, 2016, to determine whether the selected AIMS2.0 changes were appropriately authorized, tested, approved, and implemented into the production environment.

- 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.

Rick Scott
Governor

Celeste Philip, MD, MPH
Surgeon General and Secretary

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

November 17, 2016

Ms. Sherrill F. Norman, CPA
Auditor General
Room 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 audit findings and recommendations concerning the Office of the Auditor General's information technology operational audit of the *Department of Health Acquired Immune Deficiency Syndrome Information Management System*. Our response to the findings is enclosed, as required by Section 11.45(4)(d), *Florida Statutes*.

We appreciate the efforts of you and your staff in assisting to improve our operations and information systems. Please contact our Inspector General, James D. Boyd, by calling (850) 245-4141, should you have any questions.

Sincerely,

Celeste Philip, MD, MPH
Surgeon General and Secretary

CP/mhb
Enclosure

cc: James D. Boyd, CPA, MBA, Inspector General
Anna Likos, MD, MPH, Interim Deputy Secretary for Health

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

Report Number: To be determined
Report Title: *Acquired Immune Deficiency Syndrome Information Management System*
Report Date: To be determined

No.	Finding	Recommendation	Management Response	Corrective Action Plan
1.	The Department of Health (Department) had not established policies and procedures for various AIMS2.0 processes or user responsibilities, increasing the risk that tasks related to various AIMS2.0 processes and user responsibilities will not be carried out consistently and in a manner pursuant to management's expectations.	We recommend that Department management continue efforts to establish policies and procedures for AIMS2.0 processes and user responsibilities.	We concur.	**In Progress.** Projected Completion Date – March 31, 2017 The AIMS2.O *User Manual* was completed and approved by the HIV/AIDS Section Administrator August 25, 2016. The HIV/AIDS Patient Care and Data Integration teams are taking the lead to develop policy and procedure documents for the AIMS2.O application.
2.	The Department had not created application design documentation for AIMS2.0 to ensure that AIMS2.0 aligned with management's business requirements.	To help ensure that AIMS2.0 aligns with Department management's business requirements, we recommend that Department management create and maintain application design documentation.	We concur.	**In Progress.** Projected Completion Date – June 30, 2017 The HIV/AIDS Data Integration team is taking the lead to reverse engineer the AIMS2.O application in order to develop design documentation that aligns with AIMS2.0 business requirements. The program office will request the addition of a contracted business analyst to the Data Integration team to assist in developing design and other documentation as required.
3.	The Department had not established procedures for the periodic review of AIMS2.0 user access privileges and did not perform periodic reviews of access privileges.	We recommend that Department management establish procedures requiring that the authorization and appropriateness of AIMS2.0 user access privileges be periodically reviewed and ensure that such reviews are timely performed.	We concur.	**In Progress.** Projected Completion Date – November 30, 2016 Procedures for the periodic review of AIMS 2.0 user access privileges are currently being developed and documented. The HIV/AIDS Patient Care team has completed the statewide review of user access privileges and adjusted the user access rights according to the user access authorization form submitted by each user. This action was completed October 19, 2016. The HIV/AIDS Patient Care and Data Integration teams have agreed to develop and implement a system enhancement that will mark users "inactive" if there is no account activity within a six-month period.

No.	Finding	Recommendation	Management Response	Corrective Action Plan
4.	Documentation supporting authorization of access privileges for AIMS2.0 for some employees was missing or incomplete or did not match the user access privileges granted. In addition, the Department's local office for AIMS2.0 had not established written procedures for the security administration of AIMS2.0.	We recommend that Department management improve controls to ensure that applicable security administration procedures are documented and that access authorization forms are retained, complete, and commensurate with management's direction.	We concur.	**In Progress.** Projected Completion Date – January 31, 2017 The HIV/AIDS Patient Care team completed the documentation of user authorization and access privileges and updated the users account in AIMS2.O system accordingly. This was completed October 19, 2016. The user authorization and access privilege document is stored on a network folder. Additionally, the program will develop security administration procedures for AIMS2.O system in coordination with the Department's Information Security team. The HIV/AIDS Data Integration team will request the addition of a contracted Business Analyst to reverse engineer the AIMS2.O system and develop requirements and design documents.
5.	The access privileges of some AIMS2.0 users did not restrict users to only those functions appropriate and necessary for their assigned job duties.	We recommend that Department management limit user access privileges to AIMS2.0 data and IT resources to promote an appropriate separation of duties and restrict users to only those functions necessary for their assigned job duties.	We concur.	**In Progress.** Projected Completion Date – November 30, 2016 The HIV/AIDS Patient Care team reviewed all user access privileges and adjusted the privileges according to their role requested on the user access authorization form. User access forms for all AIMS users are being scanned, properly identified and stored.
6.	The Department did not timely deactivate the AIMS2.0 accounts for some former employees to prevent the former employees or others from misusing the former employees' access privileges.	We recommend that Department management ensure that the AIMS2.0 accounts of former employees are timely deactivated.	We concur.	**In Progress.** Projected Completion Date – November 30, 2016 The HIV/AIDS Patient Care team completed the review of all accounts in AIMS2.O system and deactivated the accounts for those users that did not submit user access authorization forms. The HIV/AIDS Patient Care team will receive a request by phone, email or ticket request to disable a AIMS user account. The *User Authorization* form will document the reason and inactive date. The AIMS user account will be deactivated when the *User Authorization* form is received. The process will be documented as part of Corrective Action 3 above. The HIV/AIDS Patient Care and Data Integration teams have agreed to develop and implement a system enhancement that will mark users "inactive" if there is no account activity within a six-month period.

No.	Finding	Recommendation	Management Response	Corrective Action Plan
7.	The Department had not implemented a complete system development life cycle methodology to ensure that security or functionality requirements were included throughout the development and maintenance of AIMS2.0.	We recommend that Department management establish a documented SDLC methodology to ensure that security and functional requirements are included in the maintenance of AIMS2.0.	We concur.	**In Progress.** Projected Completion Date – November 30, 2016 The HIV/AIDS Patient Care and Data Integration teams have begun to implement documented system development life cycle (SDLC) methodology for any future system enhancements and bug fixes. The HIV Support and Workflow management system will be implemented by November 20, 2016 to assist program document enhancement requests and bug reports. This feature allows management to track the enhancement or bug fix throughout the SDLC process with documentation, proper approvals and sign off after each process.
8.	The Department had not established controls to ensure that all program changes related to AIMS2.0 that had been implemented into the production environment were appropriately authorized, tested, and approved.	We recommend that Department management establish controls to ensure that only authorized, tested, and approved program changes related to AIMS2.0 are implemented into the production environment.	We concur.	**In Progress.** Projected Completion Date – November 30, 2016 The HIV Support and Workflow management system will be implemented by November 30, 2016 to assist the program in documenting the release cycles and include only authorized, tested and approved changes for promotions. This system allows management to track the enhancement or bug fix throughout the SDLC process with documentation, proper approvals and sign off after each process.
9.	Certain security controls related to user authentication, access privileges, and monitoring for AIMS2.0 and related IT resources need improvement to ensure the confidentiality, integrity, and availability of AIMS2.0 data and related IT resources.	We recommend that Department management improve certain security controls related to user authentication, access privileges, and monitoring for AIMS2.0 and related IT resources to ensure the confidentiality, integrity, and availability of AIMS2.0 data and related IT resources.	We concur.	**Completed.** The HIV Data Integration team implemented system updates specific to security controls identified during the audit process in coordination with the Department's Information Security team.