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

Florida HEALTH

Rick Scott
Governor

Celeste Philip, MD, MPH
Surgeon General and Secretary

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

May 16, 2017

Celeste Philip, MD, MPH
Surgeon General and Secretary
4052 Bald Cypress Way
Tallahassee, Florida   32399

Dear Dr. Philip:

Pursuant to Section 20.055(6)(h), *Florida Statutes*, our office is to update you on the status of corrective actions taken since November 22, 2016 when the Office of the Auditor General published its Report Number 2017-051*, Department of Health Acquired Immune Deficiency Syndrome Information Management System.* Management's assessment of the current status of corrective actions is included in the enclosed document.

We are pleased to report that at six months after publication, management has completed all corrective actions made in response to recommendations from the Office of the Auditor General.

If I may answer any questions, please let me know.

Sincerely,

James D. Boyd, CPA, MBA
Inspector General

JDB/mhb
Enclosure

cc: Kathy DuBose, Staff Director, Joint Legislative Auditing Committee
     Eric Miller, Chief Inspector General, Executive Office of the Governor
     Kelli T. Wells, MD, Deputy Secretary for Health

Florida Department of Health
Office of Inspector General
4052 Bald Cypress Way, Bin A-03 • Tallahassee, FL 32399
PHONE: 850/245-4141 • FAX: 850/413-8985
FloridaHealth.gov

PHAB **Accredited Health Department**
Public Health Accreditation Board

Report Number: 2017-051
Report Title: *Acquired Immune Deficiency Syndrome Information Management System*
Report Date: November 22, 2016
Status As Of May 16, 2017

No.	Finding	Recommendation	Corrective Action Plan	Status of 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.	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.	**Completed.** The HIV/AIDS Patient Care and Data Integration teams have developed the *System Security Administration Policies and Procedures*.
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.	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.	**Completed.** The HIV/AIDS Data Integration team added a Business Analyst to the team. The Business Analyst is tasked with developing our current business, functional, and design documents. The Business Analyst will continue to work on remaining functional requirement documents and software design documents.

No.	Finding	Recommendation	Corrective Action Plan	Status of Corrective Action Plan
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.	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.	**Completed.** The HIV/AIDS Data Integration Team developed and implemented system enhancements in support of this finding. Users were provided instructions to confirm their access by logging into the AIMS system and confirming the periodic message that appears on the dashboard. The implementation record for the periodic message and the dashboard message in the system is shown in Software Release Notes. The AIMS periodic review procedure is documented in the *System Security Administration Policies and Procedures*.
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.	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.	**Completed.** The HIV/AIDS Patient Care and Data Integration teams have developed the AIMS *System Security Administration Policies and Procedures*. Sections 4 and 5 of the document support completion of the finding. The HIV/AIDS Data Integration team continues to work on system enhancements to complement this task.

No.	Finding	Recommendation	Corrective Action Plan	Status of Corrective Action Plan
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 information technology resources to promote an appropriate separation of duties and restrict users to only those functions necessary for their assigned job duties.	The HIV/AIDS Patient Care team reviewed all user access privileges and adjusted the privileges per their role requested on the user access authorization form. User access forms for all AIMS users are being scanned, properly identified and stored.	**Completed.** The HIV/AIDS Patient Care team completed the scanning of all user access forms. Additional system enhancements in support of the *Access Request* form will include adding a field to capture the job description for all the user roles defined in the system. In addition, during the periodic review, all the users will provide an electronic consent for the correctness of their job description in the system.
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.	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.	**Completed.** The HIV/AIDS Patient Care and Data Integration teams implemented an enhancement in October 2016 to mark users "Inactive" when there is no account activity within a six-month period. The teams will now develop and implement a system enhancement that will mark users "Deleted" if there is no account activity within a 60-day period.

No.	Finding	Recommendation	Corrective Action Plan	Status of 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 Serum and System Development Life Cycle (SDLC) methodology to ensure that security and functional requirements are included in the maintenance of AIMS2.0.	The HIV/AIDS Patient Care and Data Integration teams have begun to implement the 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.	**Completed.** The HIV/AIDS Data Integration Team has adopted an Agile methodology approach for future AIMS system enhancements and system development. The team is using Microsoft Visual Studio Team Services (VSTS) as the integrated development environment to facilitate the SDLC.
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.	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.	**Completed.** The HIV/AIDS Data Integration team has implemented an Agile methodology to ensure only authorized, tested, and approved code changes are promoted to the production environment. Documentation includes project change requests, reported bugs, test cases, and release notes.
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.	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.	**Previously completed.**