STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2018-013
August 2017

DEPARTMENT OF CHILDREN AND FAMILIES

Substance Abuse and Mental Health Information System (SAMHIS)

Sherrill F. Norman, CPA
Auditor General

Secretary of the Department of Children and Families

The Department of Children and Families is established by Section 20.19, Florida Statutes. The head of the Department is the Secretary who is appointed by the Governor and subject to confirmation by the Senate. During the period of our audit, Mike Carroll served as Department Secretary.

The team leader was Chrystal Temples 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 CHILDREN AND FAMILIES

Substance Abuse and Mental Health Information System (SAMHIS)

SUMMARY

This operational audit of the Department of Children and Families (Department) focused on evaluating selected information technology (IT) controls applicable to the Substance Abuse and Mental Health Information System (SAMHIS) and included a follow-up on findings included in report No. 2015-155 that were applicable to the scope of this audit. Our audit disclosed the following:

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

Finding 2: SAMHIS did not facilitate reconciliations of client service data to the associated expenditure data recorded in the Department's and Behavioral Health Managing Entities' accounting records.

Finding 3: The Department had not established procedures for periodic reviews of SAMHIS user access privileges and did not perform such reviews during the period July 2016 through April 2017.

Finding 4: The Department's access control procedures need improvement to better ensure that access privileges granted for users of SAMHIS and the Department's network are timely deactivated when users separate from employment.

Finding 5: Certain Department security controls related to user authentication, logging and monitoring, and the protection of confidential and exempt data for SAMHIS and related IT resources need improvement.

BACKGROUND

State law[1] requires the Department of Children and Families (Department) to work in partnership with local communities to protect the vulnerable, promote strong and economically self-sufficient families, and advance personal and family recovery and resiliency. The Substance Abuse and Mental Health (SAMH) Program is responsible for the oversight of a Statewide system of care for the prevention, treatment, and recovery of children and adults with serious mental illnesses or substance abuse disorders. The Department contracts with regional organizations referred to as Behavioral Health Managing Entities (MEs) to manage the daily operational delivery of behavioral health services through a coordinated system of care. The Department contracts with seven MEs to manage these services in Florida.

The Substance Abuse and Mental Health Information System (SAMHIS) is a database used by the SAMH Program Office and the MEs to collect, store, and report data related to those (i.e., clients) receiving substance abuse and mental health services.

[1] Section 20.19, Florida Statutes.

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. Our review of SAMHIS transaction data input controls disclosed that some application input edits need improvement. Specifically, we noted that:

- Users record data regarding client seclusion and restraint information on the Seclusion and Restraint Event (SANDR) screen in SAMHIS. During a demonstration of SAMHIS, we observed that the implementation time field on the SANDR screen allowed the entry of incorrect time information, such as a value between 2401 and 2459. We further noted that SAMHIS allowed a termination date or time to be recorded that was earlier than the start date and time, which would result in a negative duration for an event.
- Department procedures[2] require MEs to identify in SAMHIS the substance (i.e., drug) that was primarily responsible for the client's admission to a State-contracted community substance abuse and mental health provider agency. Additionally, Department procedures provide that the MEs are not to record the same drug in the primary, secondary, and tertiary fields even if different routes were used by the client to administer the same drug. However, SAMHIS did not have an edit in place to prevent the entry of the same drug in the primary, secondary, and tertiary fields and, consequently, we noted instances in which the client record in SAMHIS listed the same drug in more than one of these fields.
- As also noted in our report No. 2015-155 (finding No. 4), SAMHIS lacked edit checks to prevent the entry of the same social security number (SSN) for multiple clients. Department management stated that the Department is in the process of implementing corrective action in two phases that will address the impact of duplicate SSNs in SAMHIS. Specifically, phase one was implemented on June 30, 2017, and phase two is scheduled to be completed on September 17, 2017.

The lack of adequate application input edits increases the risk that data may be compromised and inaccurately reported.

Recommendation: We recommend that Department management continue efforts to implement necessary application input edits to ensure the accuracy and validity of SAMHIS data.

Finding 2: SAMHIS Reconciliations

When multiple applications are used to capture and account for the cost of services and service payment amounts, application controls should include procedures to reconcile data among applications. Effective reconciliation procedures reasonably ensure the accuracy and completeness of the data and timely identify discrepancies that may require corrective actions. Additionally, effective monitoring procedures help ensure that reconciliations are appropriately and timely performed.

Monthly, the Department uses the Florida Accounting Information Resource Subsystem (FLAIR) to advance pay the MEs one-twelfth of the annual contract amounts. The MEs upload client service data into SAMHIS monthly. The MEs also provide the Department monthly actual expenditure reports from

[2] Department Pamphlet 155-2, *Mental Health and Substance Abuse Measurement and Data,* Chapter 6A, *Substance Abuse Admission Data Set (SA ADMSN)*.

the MEs' accounting records. The Department uses the ME monthly expenditure reports to adjust FLAIR to reflect actual expenditures. To ensure the accuracy of the data supporting the expenditures, periodic reconciliations of the MEs' accounting records data to the SAMHIS client service data, as well as periodic reconciliations of the SAMHIS client service data to the associated FLAIR expenditure data, are necessary.

As part of our audit we examined Department records and Department guidelines provided to the MEs for recording client service and expenditure data and, as similarly noted in finding No. 6 in our report No. 2015-155, we found that:

- The Department was not able to perform a complete reconciliation of SAMHIS client service data to the associated FLAIR expenditure data. Although the Department implemented a standardized expenditure report to assist in reconciling services to expenditures, made programming changes to SAMHIS to allow providers to record billed and paid amounts, and instructed MEs to collect the data, certain limitations continued to prevent a complete reconciliation. In response to our audit inquiry, Department management indicated that variations existed in the timing and basis of payments, depending on the service and contract types. Department management also stated that these issues were being reviewed and that the Financial and Service Accountability Management System (FASAMS) Project, which will result in the replacement of SAMHIS and the resolution of the reconciliation issue, would continue.
- While the Department provided to the MEs guidelines for recording and providing the Department with monthly year-to-date client service data and summarized year-to-date expenditure data by FLAIR category code, the Department had not provided to the MEs guidance for reconciling ME accounting records data to SAMHIS client service data.
- The Department did not have procedures to periodically review documentation of ME-prepared reconciliations and verify that the reconciliations were appropriately and timely performed.

Absent SAMHIS functionality to facilitate the preparation of accurate and complete reconciliations of client service data to the associated FLAIR expenditure data and the MEs' accounting records, the Department and MEs have limited ability to ensure that expenditures are accurate and complete and that any discrepancies will be timely identified and corrected. Department-established procedures for reconciling SAMHIS and FLAIR data and Department-provided guidelines for ME use when reconciling ME accounting records data to SAMHIS client service data would further promote the accuracy and completeness of the expenditure data and would provide additional assurances regarding the consistency and adequacy of ME reconciliation processes.

Recommendation: To facilitate the reconciliation of client service data to the associated expenditure data in FLAIR and ME accounting records, we recommend that Department management consider the service and payment reconciliation issues as part of the FASAMS Project. Additionally, we recommend that Department management develop procedures for reconciling client service data with the associated FLAIR expenditure data and also establish guidelines for ME use when reconciling ME accounting records to SAMHIS data. Department management should also require that Department staff periodically review documentation of the ME-prepared reconciliations to ensure that the reconciliations are appropriately and timely performed.

Finding 3: Periodic Review of Access Privileges

Agency for State Technology (AST) rules[3] 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.

As similarly noted in our report No. 2015-155 (finding No. 7), our audit procedures disclosed that during the period July 2016 through April 2017, the Department had not established procedures for, and had not performed, a periodic review of SAMHIS user access privileges. In response to our audit inquiry, Department management stated that each quarter the security officer performs a review of the User Lockout report and forwards the report to the appropriate supervisors for additional action. However, our review of the User Lockout report disclosed that only the user accounts locked out due to 60 days of inactivity were included on the report. Consequently, a user's access privileges are not reviewed unless the user has been inactive for 60 days or more.

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

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

Finding 4: Timely Deactivation of Access Privileges

AST rules[4] require each agency to manage identities and credentials for authorized devices and users and ensure that 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 when access to the information is no longer required is necessary to help prevent misuse of the access privileges. Additionally, Department policy[5] requires that appropriate Department security personnel be immediately notified when a user separates from Department employment or no longer needs SAMHIS access so that the user's access can be deactivated.

Our review of the access privileges for the six Department headquarters employees who separated from Department employment between July 1, 2016, and February 28, 2017, disclosed that two of the six former employees were SAMHIS users and that the Department did not timely deactivate the SAMHIS user account for one of the two users. Specifically, we found that the SAMHIS user account for one SAMHIS user remained active for 33 days after the employee's separation date of July 29, 2016.

In response to our audit inquiry, Department staff stated that, because an employee's network account is deactivated the same day as their separation and network access is required to access SAMHIS, there

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

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

[5] *SAMHIS Security Policy*.

was no risk of the former employee accessing SAMHIS after separation from Department employment. However, our review disclosed that the former employee's network account was not deactivated until August 9, 2016, 11 days after the employee's separation from Department employment. We also noted that, because access to SAMHIS requires a user to separately log on to SAMHIS once the user has logged on to the network, the possibility exists that an individual who has successfully logged on to the network could inappropriately use the logon credentials of a former employee to log on to SAMHIS, thus circumventing the controls related to the deactivation of the former employee's network access.

Through our review of Department documentation, we determined that the former employee's SAMHIS user account had not been used subsequent to the date of employment separation. A similar finding was noted in our report No. 2015-155 (finding No. 7).

Timely deactivation of SAMHIS and network user account access privileges upon an employee's separation from Department employment reduces the risk that unauthorized SAMHIS or network use by the former employee or others may occur.

Recommendation: We recommend that Department management improve procedures to ensure that the SAMHIS and network user accounts of former employees are timely deactivated.

Finding 5: 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 SAMHIS data and related IT resources. However, we have notified appropriate Department management of the specific issues.

The lack of appropriate SAMHIS 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 SAMHIS data and related IT resources may be compromised.

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

PRIOR AUDIT FOLLOW-UP

As noted in Findings 1 through 4, Department management had taken corrective action to partially address finding No. 4 in our report No. 2015-155; however, Department management had not taken corrective actions to address finding No. 6 and the applicable portions of finding No. 7 included in that report.

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 January 2017 through April 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 IT controls applicable to SAMHIS during the period July 2016 through April 2017. The audit included selected business process application and interface controls and selected application-level general controls over logical access and change management. The audit also included selected application-level general controls applicable to SAMHIS that related to the deficiencies disclosed in our report No. 2015-155. 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; and the safeguarding of IT resources.
- To determine whether management had corrected, or was in the process of correcting, all deficiencies disclosed in audit report No. 2015-155 that were applicable to the scope of this audit.
- 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 SAMHIS, including the:
  - Background of SAMHIS, including the purpose and goals involving financial, operations, and compliance requirements.
  - Business process flows of key sources of data input, including interfaces, and key types of application data output related to SAMHIS.
  - Application change management process for SAMHIS, including identification of policies and procedures for program change control.
  - Procedures for user account management processes for authorizing, creating, modifying, and revoking SAMHIS user accounts.
  - Periodic review of access privileges for SAMHIS user accounts.
  - Status of Department efforts to identify and investigate duplicate client social security numbers in SAMHIS and implement edits in SAMHIS to prevent the input of the same social security number for multiple clients.
- Evaluated SAMHIS transaction data input controls related to ME data and other data input by Department employees. Specifically, we:
  - Examined the online field edits on the Seclusion and Restraint Event screen used by MEs for manual data input to verify that ME data input entry is validated and effectively controlled. On February 16, 2017, observed Department personnel entering invalid data to determine whether the online edits built into SAMHIS were in place and displayed appropriate error messages.
  - Examined January 20, 2017, error count reports used by Department staff to monitor data error counts for specific error types from the data submitted by the MEs to evaluate the adequacy of the Department's data accuracy monitoring procedures.
  - Examined January 20, 2017, acceptance rate reports used by Department staff to monitor the percentage of records submitted that did not have an error detection event (acceptance rate) for the data submitted by the MEs to evaluate the adequacy of the Department's monitoring procedures for ME acceptance rates.
  - Examined the SAMHIS programming code that performs error checking functions to detect errors or irregularities in the data files that the MEs upload to SAMHIS and reviewed documents the Department provides to MEs explaining the returned error codes to evaluate the adequacy of the Department's monitoring procedures for data upload accuracy.
  - Reviewed Department Pamphlet 155-2, *Mental Health and Substance Abuse Measurement and Data,* to evaluate Department guidance provided to MEs regarding the meaning of numeric error codes applied to records listed in an error file so that errors could be promptly investigated and data appropriately resubmitted for processing.

- Evaluated interface processing procedures for data uploaded into SAMHIS from ME client systems. Specifically, we:
    - Examined on February 16, 2017, the file history upload screen within SAMHIS that provides the MEs immediate feedback on the processing results of the data uploaded to SAMHIS to evaluate the adequacy of the information to facilitate the submission of accurate data.
    - Examined Department documentation that identified responsibilities related to interface processing between the Department and the MEs, including the type and format of provider data submitted, when the data is submitted, who submits the data, and who makes data error corrections to evaluate whether the Department has appropriately assigned interface processing responsibilities.
    - Examined the *2016-17 CBC-ME Financial Monitoring Tool Desk Review* used by Department staff to conduct desk review monitoring of the MEs and a reconciliation spreadsheet and related guidelines to determine whether the Department established procedures or guidelines for reconciling interfaced data between ME systems and SAMHIS, ME systems and the State's accounting system (FLAIR), and SAMHIS and FLAIR, and for periodically reviewing ME-prepared reconciliations.
    - Reviewed the agenda for the March 2, 2017, Monthly SAMH Contract Manager Call, Tableau and other Quality Data Improvement Project reports as of January 20, 2017, and Department management e-mail responses to determine whether the data integrity concerns previously identified in the SAMHIS Upload History Report were resolved.
    - Examined SAMHIS programming code to determine whether automated programmed controls were in place to prevent data files from being processed more than once.
- Evaluated selected SAMHIS transaction data output controls related to data reporting for Federal, State, regional, and provider-level requirements. Specifically, we:
    - Examined selected critical output reports (i.e., Federal Reporting and Quality Data Improvement Project reports) generated during the period July 2016 through April 2017 and related procedures to determine whether system generated outputs and reports are reviewed to reasonably assure the integrity of production data and transaction processing.
- Evaluated application access controls related to SAMHIS. Specifically, we:
    - Reviewed the *SAMHIS Security Policy* to determine whether adequate procedures were in place for creating, modifying, and revoking user access privileges.
    - Reviewed the *SAMHIS Security Policy* and other documentation to determine whether adequate procedures were in place for periodically reviewing SAMHIS access privileges.
    - Reviewed Department policies and a list of active users to determine whether access for SAMHIS users was role-based.
    - Determined the timeliness of SAMHIS access deactivations for employees that had SAMHIS access and separated from Department employment between July 1, 2016, and February 28, 2017.
- Evaluated access controls designed to protect sensitive system resources.
- Evaluated the effectiveness of logging and monitoring controls related to SAMHIS IT resources.
- Evaluated identification and authentication controls related to SAMHIS.
- Evaluated program change management controls related to SAMHIS. Specifically, we:
    - Reviewed Department procedures to determine whether the Department maintained a current program change management procedure for SAMHIS.

- Examined 5 of 15 program change requests completed between July 1, 2016, and January 26, 2017, to determine whether SAMHIS program changes were appropriately authorized, tested, approved, and implemented into production.

- 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 this 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

State of Florida
Department of Children and Families

Rick Scott
Governor

Mike Carroll
Secretary

August 9, 2017

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

Dear Ms. Norman:

This letter is in response to the preliminary and tentative audit findings and recommendations issued to the Department of Children and Families on July 7. The findings and recommendations were related to an information technology operational audit of the Department of Children and Families Substance Abuse and Mental Health Information System (SAMHIS).

In response to findings contained in the March 2015 Operational Audit Report No. 2015-155, Oversight of Substance Abuse and Mental Health Services, the Department received funding to pursue the development of a replacement data system for tracking and managing financial and service data related to Department funded behavioral healthcare services. The Department anticipates awarding a contract for the development of the new system, the Financial and Services Accountability Management System (FASAMS) by September 30, 2017. Recommendations discussed in the July 7 preliminary and tentative audit findings will be incorporated into FASAMS.

Information regarding the Department's ongoing data improvements is included below.

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

The audit determined that SAMHIS data entry screens and File Transfer Protocol data submission processes allow for data values outside of standard ranges such as invalid times or terminating dates that precede initiation dates.

1317 Winewood Boulevard, Tallahassee, Florida 32399-0700

Mission: Work in Partnership with Local Communities to Protect the Vulnerable, Promote Strong and Economically Self-Sufficient Families, and Advance Personal and Family Recovery and Resiliency

The Department will include the deployment of the Master Client Index (MCI) process, planned enhancements to SAMHIS, and incorporate additional validation rules in FASAMS.

The MCI process will assign a unique identifier (UID) to each person served by SAMH funds based on proven methodologies built into the Department's Office of Economic Self-Sufficiency's FLORIDA system. As of July 1, 2017, more than four million UIDs, out of an approximate total of five million, have been assigned to SAMHIS demographic records via the MCI process. An additional one million demographic records are anticipated to be resolved by October 31, 2017, once an automated UID process is deployed.

Data validation edits to SAMHIS to prevent problems identified during the audit are being reviewed and prioritized for development either in SAMHIS or in FASAMS.

Finding 2: SAMHIS did not facilitate reconciliations of client service data to the associated expenditure data recorded in the Department's and Behavioral Health Managing Entities' accounting records.

As indicated in this report, finding No. 2 is similar to finding No. 6 contained in the March 2015 Operational Audit Report No. 2015-155, Oversight of Substance Abuse and Mental Health Services. Functionality to define core business rules for linking services and financial data will be added to the future FASAMS system, and complete documentation will be provided to the Managing Entities (ME) and other data submitters to ensure financial and service accountability.

In the interim, the Department has added functionality to both its existing data collection and expenditure reconciliation models. SAMHIS functionality has been expanded to better connect SAMHIS collected service/encounter data with financial data from internal and external data systems. Simultaneously, supporting documentation for the Managing Entity monthly invoicing and year-end reconciliation process has been expanded to capture provider-level detail connecting service events to fund sources. While this approach still requires a manual reconciliation of reports generated across multiple systems, it provides significant additional validation pending the implementation of an integrated data and financial management system.

The Department will establish procedures to conduct monthly reviews of ME expenditure data through the Department's financial accountability office and will directly incorporate SAMH service event data from the MEs for validation and reconciliation.

Finding 3: The Department has not established and implemented procedures for periodic reviews of SAMHIS user access privileges.

By the fifth working day of each month, ME Data Liaisons will check the roles of their staff and subcontractor staff with SAMHIS access to ensure that continued SAMHIS access is needed, and that roles are appropriate for the employee's current job responsibilities. Using an Ad Hoc Active User Report to check the last SAMHIS login date for all staff and subcontractor staff, the Data Liaison shall complete a Database Access Request Form requesting deactivation for each user with 60 or more days of SAMHIS inactivity, and submit the form to the SAMH Data Unit by the tenth of each month.

Finding 4: The Department's access control procedures need improvement to better ensure that access privileges granted for users of SAMHIS and the Department's network are timely deactivated when users separate from employment.

To ensure that SAMH headquarters employee SAMHIS and network access is revoked upon separation, the SAMH Human Relations liaison will email the Data Unit security staff at least one day prior for all anticipated separations. For unanticipated separations, the SAMH Human Relations liaison will email the Data Unit security staff as soon as separation has been completed. In both cases, the employee's SAMHIS and network access will be revoked immediately following notification.

Finding 5: Certain Department security controls related to user authentication, logging and monitoring, and the protection of confidential and exempt data for SAMHIS and related IT resources need improvement.

The audit revealed that the SAMHIS security controls need improvement and provided recommendations on how to improve the security of SAMHIS data. The Department agrees with the findings. The Department is evaluating which solutions will be implemented in SAMHIS and which will be incorporated into the future FASAMS system.

Thank you for the opportunity to provide feedback.

Sincerely,

Mike Carroll
Secretary