REPORT NO. 2011-057
DECEMBER 2010

AGENCY FOR HEALTH CARE ADMINISTRATION

FLORIDA MEDICAID MANAGEMENT INFORMATION SYSTEM (FMMIS)

AND

DECISION SUPPORT SYSTEM (DSS)

Information Technology Operational Audit

For the Period
July 1, 2009, Through June 30, 2010,
and Selected Actions Through September 28, 2010

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

SECRETARY OF HEALTH CARE ADMINISTRATION

Pursuant to Section 20.42(2), Florida Statutes, the Secretary of Health Care Administration is appointed by the Governor, subject to confirmation by the Senate. During the audit period, the following individuals served as Secretary:

Secretary	Dates of Service
Holly Benson	February 25, 2008, through October 28, 2009
Thomas W. Arnold	October 29, 2009, through August 31, 2010
Elizabeth Dudek	Interim Secretary from August 31, 2010

The audit team leader was Brenda Shiner, CISA, and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, by e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 487-9024; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

AGENCY FOR HEALTH CARE ADMINISTRATION

Florida Medicaid Management Information System (FMMIS)

and

Decision Support System (DSS)

SUMMARY

Sections 409.901(2) and (15), Florida Statutes, designate the Agency for Health Care Administration (Agency) as the single State agency that administers or supervises the administration of the State Medicaid plan under Federal law. HP Enterprise Services, LLC (HP), formerly known as Electronic Data Systems, LLC, became the Medicaid fiscal agent on June 26, 2008, and developed and operates the Florida Medicaid Management Information System (FMMIS) and Decision Support System (DSS). FMMIS is used to enroll providers, process Medicaid claims, adjudicate claims, and reimburse providers. FMMIS data is imported into DSS to enable efficient reporting and data analysis. The Medicaid Program is highly dependent on the security, integrity, and proper functioning of FMMIS and DSS.

Our audit focused on evaluating the effectiveness of selected information technology (IT) controls applicable to FMMIS and DSS during the period July 1, 2009, through June 30, 2010, and selected actions through September 28, 2010. We also determined the status of corrective actions regarding audit findings included in our report No. 2010-025. Our audit disclosed numerous instances where FMMIS and DSS IT controls were deficient or needed improvement. These control issues limit the Agency's assurance of the security and reliability of Medicaid Program data and the Agency's accountability over the Medicaid Program. Our findings are summarized below:

Access Controls

Finding No. 1: **The Agency and HP lacked appropriate access control documentation to demonstrate the business justification for access privileges granted within FMMIS, DSS, and the related system software. Similar issues were noted in our report No. 2010-025.**

Finding No. 2: **The access privileges of some employees and contractors were not appropriate for their job responsibilities. Similar issues were noted in our report No. 2010-025.**

Finding No. 3: **Some former contractor access privileges were not timely disabled. Similar issues were noted in our report No. 2010-025.**

Finding No. 4: **Contrary to the requirements of the Department of State General Records Schedule for retention of access control records, the Agency did not retain some FMMIS and DSS access control records for the server operating systems.**

Finding No. 5: **Except for HP quarterly reviews of application access privileges, neither the Agency nor HP performed periodic reviews of the appropriateness of access privileges. A similar issue was noted in our report No. 2010-025.**

Finding No. 6: **As also noted in our report No. 2010-025, generic user identifications (IDs) for database administration were being shared by contractor staff.**

Finding No. 7: **Certain security controls were deficient in the areas of user authentication, session controls, and logging of system activity. Similar issues were noted in connection with our report No. 2010-025.**

Other IT Controls

Finding No. 8: **Program and data change controls for FMMIS and DSS needed improvement. Similar issues were noted in our report No. 2010-025.**

Finding No. 9: **In some instances, customer service requests (CSRs) to correct recipient eligibility processing errors were not analyzed in a timely manner to determine the impact of the processing errors and to ensure that CSRs were effectively prioritized.**

Finding No. 10: Contrary to the HP Resolutions Procedures Manual, HP was not performing quality control reviews to ensure that claims subject to manual resolution procedures were processed accurately and correctly.

BACKGROUND

Medicaid is a partnership between the State and Federal Government to provide health coverage for selected categories of people with low incomes. Section 409.902, Florida Statutes, designates the Agency as the single State agency authorized to make payments for medical assistance and related services and provides that those payments shall only be made on behalf of eligible individuals and only to qualified providers in accordance with Title XIX of the Federal Social Security Act. Section 409.902, Florida Statutes, further states that the Department of Children and Family Services (DCFS) is responsible for Medicaid eligibility determinations. DCFS communicates recipient eligibility information to FMMIS on a daily basis.

The Bureau of Medicaid Contract Management within the Division of Medicaid manages the contract for HP (the fiscal agent) to maintain FMMIS, enroll providers, and process claims for payment. In addition, the Bureau of Medicaid Contract Management, among other duties, oversees claims resolution and provider enrollment policies and resolves Medicaid recipient eligibility file problems in FMMIS. FMMIS data is imported into DSS to enable efficient reporting and data analysis. The Agency uses FMMIS and DSS for Medicaid Program oversight and analysis.

The Agency and HP were each responsible for security administration functions for their respective users of FMMIS. Server operating system and database user account management was performed by HP system and database administrators. HP also managed the development and promotion of FMMIS and DSS program changes using change control software.

FINDINGS AND RECOMMENDATIONS

The Medicaid Program is highly dependent on the security, integrity, and proper functioning of FMMIS and DSS to ensure the accurate payment of Medicaid benefits in accordance with Federal and State law and to facilitate timely and accurate reporting for Federal oversight purposes. Medicaid Program payments processed and paid by the Agency during the 2009-10 fiscal year totaled approximately $15 billion. In addition, FMMIS and DSS contain significant confidential information, including, for example, Medicaid recipient names, dates of birth, social security numbers, and medical services received. Accordingly, effective IT controls over FMMIS and DSS are critical.

Our audit disclosed numerous instances where IT controls applicable to FMMIS and DSS were deficient or needed improvement as discussed in the following paragraphs.

Access Controls

Finding No. 1: Access Control Documentation

Effective security controls include logical (electronic) access controls that limit user access privileges to only the data and IT resources that are needed to perform authorized job duties. Access controls include, among other things, the use of access authorization forms to document the access privileges that have been authorized by management for system users to be granted. Maintaining such documentation helps to ensure that only authorized access privileges are assigned to users.

Our audit disclosed that some Agency and HP access control documentation was missing or incomplete. Similar issues were noted in our report No. 2010-025. Specifically:

- HP was unable to provide documentation of the correlation of access roles for the FMMIS and DSS server operating systems with specified job functions.
- HP was unable to provide adequate documentation of the business justification (on either the access request forms or in the Role Definition by Position document created to correlate job positions with FMMIS user roles for application-level access) for FMMIS user roles granted to 13 of 19 user accounts belonging to HP employees included in our sample. Specifically, HP was unable to provide any authorization forms for 4 of the 13 user accounts and 9 user accounts did not have one or more of the assigned user roles specified on the authorization forms. Also, for 1 of the 9 user accounts, while the user roles were specified on the authorization form, the business justification was missing. We also noted that 5 of the 13 user accounts belonged to employees with job positions that were not listed on the Role Definition by Position document created to correlate job positions with FMMIS user roles. Additionally, 2 of the user roles assigned to some users included in our sample were not listed on the Role Definition by Position document.
- The Agency was unable to provide authorization forms for two of nine FMMIS user accounts belonging to Agency employees included in our sample.
- HP was unable to provide authorization forms for 25 of 48 user accounts included in our sample with access to the server operating systems. In response to audit inquiry, HP staff indicated that missing authorization forms were for employees granted access before implementation of FMMIS and DSS and those forms were no longer available. For the remaining 23 user accounts included in our sample, we inspected the authorization forms provided to us to determine if access was authorized. For 18 of 23 user accounts, the forms lacked the authorizations for one or more of the server user roles assigned to the user accounts.
- HP was unable to provide the access authorization form for 1 of 30 database user accounts included in our sample. For the remaining 29 user accounts included in our sample, we inspected the authorization forms provided to us to determine if access was authorized. For 4 of the 29 user accounts, the forms lacked the authorizations for 1 or more access privileges assigned to the accounts.
- HP was unable to provide the access authorization form for 1 of 27 user accounts included in our sample with access privileges to the program change management software. For the remaining 26 user accounts included in our sample, we inspected the authorization forms provided to us to determine if access was authorized. For 21 of the 26 user accounts, the forms lacked the authorizations for one or more access privileges assigned to the user accounts.

Absent the above-described documentation, the Agency and HP could not demonstrate the business justifications for access privileges granted within the FMMIS and DSS applications, server operating systems, database, and program change management software. These conditions limit the Agency's ability to control and monitor the appropriateness of access controls in protecting the confidentiality, integrity, and availability of data and IT resources.

Recommendation: The Agency, together with HP, should improve its procedures for user account management by maintaining adequate documentation of the authorizations and business justifications for the assignment of user access privileges.

Finding No. 2: Appropriateness of Access Privileges

Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, and destruction. Our audit disclosed instances where access privileges were inconsistent with employee or contractor job responsibilities, jeopardizing the confidentiality, integrity, and availability of data and IT resources. Specifically:

- For 7 of 19 contractors included in our sample with FMMIS user accounts, the access granted included one or more unnecessary user roles. In response to audit inquiry, HP staff stated that inappropriate access for these 7 FMMIS user accounts would be revoked.
- For 2 of 9 Agency employees included in our sample with FMMIS user accounts, the assigned user roles were inappropriate and allowed access privileges to update recipient data within FMMIS. In response to audit inquiry, Agency user account administration staff stated that 1 of the 2 user accounts was inadvertently assigned the inappropriate user role on May 11, 2009. Agency staff provided documentation showing that this account was last used on May 12, 2009, and that the inappropriate role was removed on June 22, 2010. For the other user account, Agency user account administration staff stated that the assignment of unnecessary roles occurred as a result of defined procedures not being followed. On June 23, 2010, Agency staff further stated that the unnecessary roles for the employee were removed.
- For 5 of 48 contractors included in our sample, access to the server operating systems was not necessary for their job responsibilities. HP provided documentation showing that the inappropriate access privileges for 2 of the contractors were removed on June 18, 2010. On August 10, 2010, in response to audit inquiry, HP staff stated that the inappropriate access was removed for the remaining 3 contractors. A similar issue was noted in our report No. 2010-025.
- For 13 of 30 contractors included in our sample, access to the database was not necessary for their job responsibilities. On August 3, 2010, in response to audit inquiry, HP staff stated that the inappropriate access was removed. HP staff also stated that, since the issuance of our report No. 2010-025, the form used to request database access had been updated to better document access authorization; however, there were instances whereby access privileges to the database were being requested in error. HP staff further stated that they were working to revise the form to make it clearer.
- For 19 of 27 contractors included in our sample, access to the program change management software was not necessary for their job responsibilities. Additionally, 14 of 27 contractors had the ability to both modify source program code and move the changes into the production environment without detection, contrary to an appropriate separation of duties. Similar issues were noted in our report No. 2010-025. In response to audit inquiry, HP staff stated that the inappropriate access was removed on August 10, 2010.

Recommendation: The Agency and HP should review, and adjust as appropriate, the above-described access privileges to limit access privileges to only what is needed to perform job responsibilities.

Finding No. 3: Timely Disabling of Access Privileges

Effective access controls include provisions for the timely disabling of contractor access privileges when contract terminations occur. Prompt action is necessary to ensure that the access privileges are not misused by the former contractor or others.

HP had established policies for disabling access privileges upon the termination of contractors from the Florida Medicaid contract. According to the FMMIS/DSS/Fiscal Agent Implementation HIPAA Security Policy and Procedures Manual (HIPAA Manual), access must be terminated by the end of the last business day when the employment ends, or when job responsibilities are modified to the extent that access requirements end or change. However, our audit disclosed that, contrary to HP policy, certain former contractors retained access to FMMIS and DSS applications, server operating systems, databases, and change management software after their dates of termination from the Florida Medicaid contract. Under these conditions, the risk is increased that the access privileges could be misused by the former contractors or others. Similar issues were noted in our report No. 2010-025. Specifically:

- Eight former contractors retained access privileges to the server operating systems after their dates of termination from the Florida Medicaid contract. For two of the eight contractors, HP staff could not provide their dates of termination or the length of time the access remained active after termination. The remaining six contractors

retained active access privileges to the server operating systems for at least between 260 and 732 days after their dates of termination. In response to audit inquiry, HP staff provided evidence that the access privileges had not been used to access FMMIS and DSS after termination for two of the former contractors. One former contractor accessed the server operating system 22 days after termination. Upon audit request, HP staff could not provide the dates the access privileges were last used by three of the former contractors.

- Two former contractors retained access privileges to the FMMIS and DSS databases after their dates of termination from the Florida Medicaid contract. Their database access privileges remained active for 98 and 145 days, respectively, after their dates of termination. Upon audit request, HP staff could not provide the dates the two former contractors' access privileges were last used.
- Twenty-eight former contractors retained access privileges to the program change management software after their dates of termination from the Florida Medicaid contract. For 2 of the 28 former contractors, HP staff could not provide their dates of termination or the length of time the access remained active after termination. The remaining 26 former contractors retained active access privileges for between 228 to 1,284 days after their dates of termination. Upon audit request, HP staff could not provide the dates the former contractors' access privileges were last used to access the program change management system. However, 19 of the former contractors had logged on to the server that allowed access to the program change management software after termination. In response to audit inquiry, HP stated that this server was a shared development server and was used for other HP projects as well as FMMIS development. HP staff also stated on August 10, 2010, that the access privileges for the former contractors were removed.
- Three former contractors retained user access privileges to the FMMIS application after their dates of termination from the Florida Medicaid contract. Although the access privileges associated with the former contractors were identified through HP's periodic review of FMMIS user access and the access privileges were disabled on May 28, 2010, the former contractors retained their access privileges between 148 and 574 days after termination. In response to audit inquiry, HP staff indicated that, because the user accounts had been disabled, HP could not view the historical activity to determine whether the access privileges had been used after the termination.

Recommendation: The Agency should work with HP to ensure that the access privileges of former contractors are timely disabled to minimize the risk that data and IT resources could be misused by the former contractors or others.

Finding No. 4: Access Control Records Retention

State of Florida, General Records Schedule GS1-SL for State and Local Government Agencies (General Records Schedule), revised by the Department of State effective September 2007, provides that access control records must be retained for one anniversary year after superseded or after the employee separates from employment.

HP did not retain access control records for eight users with access privileges to the server operating systems, contrary to the requirements of the General Records Schedule. Without adequate retention of access control records, the risk increases that the Agency may not have sufficient documentation to assist in future investigations of security incidents, should they occur, and would not be in compliance with the State's record retention requirements.

Recommendation: The Agency should ensure that access control records are retained as required by the General Records Schedule.

Finding No. 5: Periodic Review of Access Privileges

Periodic reviews of user access privileges help ensure that user access privileges remain appropriate. As also noted in our report No. 2010-025, the Agency did not perform periodic reviews of the appropriateness of employee user access privileges for the FMMIS and DSS applications.

In December 2009, HP began performing quarterly reviews of contractor access privileges for the FMMIS and DSS applications. However, as similarly noted in our report No. 2010-025, HP had not performed periodic reviews as of April 8, 2010, of the appropriateness of access privileges within the server operating systems, databases, or program change management software. The inappropriate access privileges disclosed in Finding Nos. 2 and 3 indicate a need for a periodic review by HP of access privileges within the server operating systems, databases, and program change management software and an increased review of application access privileges. Without timely detection and disabling or adjusting of inappropriate access privileges, the risk is increased of unauthorized disclosure, modification, and destruction of data and IT resources.

In response to audit inquiry, HP staff indicated that a periodic review of access privileges was conducted for selected servers on May 18, 2010. Additionally, Agency staff indicated a corrective action plan was established on March 25, 2010, to help ensure that periodic reviews of access privileges by HP are performed in the future.

Recommendation: The Agency should ensure that periodic reviews are conducted of the ongoing appropriateness of access privileges for the FMMIS and DSS applications, server operating systems, databases, and program change management software to facilitate the timely detection and correction of excessive or unnecessary capabilities.

Finding No. 6: User Identification

The effectiveness of access controls is dependent, in part, on the ability to uniquely identify system users. Unique identification of individual users assists in the assignment of access privileges and provides a mechanism for attributing system actions to the responsible user.

As also noted in our report No. 2010-025, HP used generic user IDs for database administration for the FMMIS and DSS databases. On September 28, 2010, in response to audit inquiry, Agency staff provided a list of 17 database administrators who shared the generic user IDs. Database administration access privileges provide, among other capabilities, the capability to change data with utility software bypassing normal application edits and controls. Without the ability to uniquely identify database administrators, the ability of the Agency and HP to establish accountability for database administration actions is limited.

Recommendation: The Agency should require HP to assign unique user IDs to all individual users authorized to perform database administration functions for FMMIS and DSS.

Finding No. 7: Other Security Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain Agency security controls that were deficient in the areas of user authentication, session controls, and logging of system activity. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising Agency data and IT resources. However, we have notified appropriate Agency management of the specific issues. These issues were also noted in connection with our report No. 2010-025. Without adequate security controls in the areas of user authentication, session controls, and logging of system activity, the confidentiality, integrity, and availability

of data and IT resources may have been compromised, increasing the risk that Agency data and IT resources may have been subject to improper disclosure, modification, or destruction.

Recommendation: The Agency should implement appropriate security controls in the areas of user authentication, session controls, and logging of system activity to ensure the continued confidentiality, integrity, and availability of Agency data and IT resources.

Other IT Controls

Finding No. 8: Program Change Controls

Effective program change controls are intended to ensure that all program changes are properly authorized, tested, approved for implementation, and documented. Our audit disclosed aspects of the Agency's program change controls for FMMIS and DSS that needed improvement, increasing the risk that unauthorized or erroneous program changes could be implemented into the production environment without timely detection, jeopardizing the ongoing integrity of FMMIS and DSS. These issues were also noted in our report No. 2010-025. Specifically:

- According to Agency staff, program changes were to be implemented and documented within production software releases. However, we identified instances where program changes were moved into the production environment without being documented as part of a production software release. Under these conditions, it could be more difficult for Agency management to track the changes made and ensure that the changes were approved prior to implementation.
- The program change management software used by HP did not provide automatic logging and reporting of program changes moved into the production environment, limiting Agency management's ability to ensure that all program changes were authorized.

Additionally, our inspection of HP program change management records for 30 FMMIS program changes disclosed instances where authorization for programming work, testing of program changes, and approval to implement program changes either were not documented or were documented as having not been performed in an appropriate sequence. Similar issues were noted in our report No. 2010-025. Specifically:

- According to FMMIS change control procedures, Agency management authorization was required for program changes other than those to correct programming or processing defects. However, Agency management authorization was lacking for 2 of 27 program changes that were made for purposes other than correcting defects.
- For 1 change, the date that programmer testing was completed preceded the date that the program change was coded.
- FMMIS change control procedures provided that program changes were to be independently tested and approved by HP business analysts. However, the business analyst testing and approval of 2 program changes was documented as having occurred before the programmer completed coding or testing the program changes.
- Agency management approval to implement 2 program changes was documented as having occurred before the programmer completed coding or testing the program changes.

Recommendation: The Agency, with the assistance of HP as applicable, should accurately document and enforce effective program change controls that provide for appropriate authorization, timely testing, and approval of changes. Additionally, to ensure that only authorized and properly functioning changes are made to FMMIS and DSS and implemented in a consistent manner pursuant to management's expectations, the Agency should log and review program changes that are moved into the production environment.

Finding No. 9: Prioritizing Customer Service Requests

Effective program change controls include procedures to ensure that all requests for changes are assessed in a structured way to determine the impact on the operational system and its functionality. As previously discussed in the Background section of this report, although AHCA was responsible for administering the Medicaid Program, recipient eligibility was determined by DCFS, which communicated recipient eligibility information to FMMIS through various daily files. These daily files included eligibility information originating from both the DCFS Florida Online Recipient Integrated Data Access (FLORIDA) System and the United States Social Security Administration. These daily files provided FMMIS with data on newly eligible recipients and changes to existing recipients including terminations of eligibility spans resulting from changes in eligibility status.

Because of two processing errors, transactions to close eligibility during the daily process were not always processed through FMMIS in a timely manner. Although customer service requests (CSRs) were written to address these processing errors, according to Agency staff within the Recipient File Management Unit, staff resources were not available to research the impact of the processing errors. Without this information, Agency Systems staff within the Bureau of Medicaid Contract Management stated that, not knowing the impact of the processing errors, they could not assign priorities to the CSRs effectively. Without timely research and review of documented FMMIS processing errors related to recipient eligibility by the Recipient File Management Unit, the risk is increased that claims for ineligible recipients will be paid.

Bureau of Medicaid Contract Management staff stated that, as of April 2010, an additional 18 HP staff had been added to the Florida Medicaid contract to help work the existing change orders and address the ongoing changes required for FMMIS. Additionally, as of June 4, 2010, Agency Systems staff had approved two change orders to correct the two processing errors and HP had begun analyzing the change orders.

Recommendation: The Agency should ensure that CSRs are adequately researched and prioritized to ensure that recipient eligibility processing errors are resolved in a timely manner.

Finding No. 10: Claims Resolution Quality Reviews

Transaction data processing controls and related user controls help ensure the completeness, accuracy, validity, and confidentiality of data as the data gets processed within an application. Such controls include adequate review and follow-up of error overrides to ensure that data is accurately processed.

According to the HP Resolutions Procedures Manual (Manual), the fiscal agent's Resolutions Department, based on Agency policy, was to resolve claims that had been suspended in FMMIS by either correcting the data on the claim record to match the claim or overriding the suspension by forcing the payment to be processed or forcing the denial of the claim. The Manual further stated that the claims support supervisor or designee was to conduct a quality control (QC) review of a random sample of 20 claims from each resolutions team member to determine whether such claims were processed accurately and correctly. The results of the QC review process were to be provided to the resolutions team members so that recurring errors could be prevented.

In response to audit inquiry, HP staff stated that the QC reviews of claims required by the Manual were no longer performed because of organizational changes that occurred in the Resolutions Department. HP staff also stated that another procedure performed by HP's Quality Assurance staff to monitor the timeliness of claims resolutions processing was in place. However, this procedure did not ensure that claims subject to manual resolution procedures were processed accurately and correctly. Without QC reviews of the claims resolution process, including overrides, the risk is increased that claims will be processed incorrectly.

Recommendation: The Agency should ensure that HP reinstates its claims resolution quality control reviews to provide assurance that claims subject to manual resolution are processed accurately and correctly by the Resolutions Department.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Agency had taken corrective actions for findings included in our report No. 2010-025.

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 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 our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of this IT operational audit were to determine the effectiveness of selected IT controls applicable to FMMIS and DSS 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. An additional objective was to determine the extent to which the Agency corrected, or was in the process of correcting, deficiencies disclosed in our report No. 2010-025.

The scope of our audit focused on evaluating selected IT controls applicable to FMMIS and DSS during the period July 1, 2009, through June 30, 2010, and selected actions through September 28, 2010. Other aspects of FMMIS functionality will be addressed in our forthcoming audits of compliance with Federal laws, rules and regulations and operational audits regarding selected Medicaid payment types.

In conducting our audit, we:

- Interviewed Agency personnel and HP contractors.
- Obtained an understanding of FMMIS and DSS, including system purpose, goals, and compliance requirements; the basic data and business processing flows for the claims processing and the recipient eligibility subsystems; system maintenance and development; and IT organizational structure and management.
- Obtained an understanding of the FMMIS and DSS computing platform and related software.
- Obtained an understanding of FMMIS application controls, including input, processing, output, and user controls related to claims processing and recipient eligibility processing.

- Obtained an understanding of the logical access controls for FMMIS and DSS including user account administration.
- Observed, tested, and evaluated key processes and procedures related to the logical access controls for FMMIS and DSS, including user account administration procedures, access authorization, appropriateness of user access, timely removal of access privileges, periodic review of user access privileges, and the adequacy of password controls related to FMMIS and DSS.
- Evaluated the effectiveness of the key processes and procedures related to the Agency's Federal certification process for FMMIS.
- Observed, tested, and evaluated the effectiveness of selected controls related to the Agency's program change control process for making application program changes to FMMIS and DSS.
- Observed, tested, and evaluated the effectiveness of selected controls over the testing, approval, and documentation of FMMIS and DSS direct data changes.
- Observed, tested, and evaluated the effectiveness of selected controls over the loading of FMMIS data into DSS.
- Evaluated the effectiveness of selected controls over the processing of claims overrides.
- Observed, tested, and evaluated the effectiveness of selected input and processing controls for FMMIS.

AUTHORITY

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.

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

In a letter dated November 23, 2010, the Secretary provided responses to our preliminary and tentative findings. This letter is included at the end of this report as EXHIBIT A.

EXHIBIT A
MANAGEMENT'S RESPONSE

CHARLIE CRIST
GOVERNOR

Better Health Care for all Floridians

ELIZABETH DUDEK
INTERIM SECRETARY

November 23, 2010

David W. Martin, CPA
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Martin:

Thank you for the opportunity to respond to the preliminary and tentative audit finding and recommendations from the Information Technology Audit of the Agency for Health Care Administration, Florida Medicaid Management Information System (FMMIS) and Decision Support System (DSS), for the period July 1, 2009 through June 30, 2010 and selected actions through September 28, 2010. We appreciate the efforts of your staff and have included our response to the recommendation noted in your report. The Agency continuously looks for opportunities to improve operations and is committed to providing cost-effective and efficient health care services to the citizens of Florida.

In accordance with your request, we have emailed you the preliminary and tentative findings document with our response incorporated therein. If you have any questions regarding our response, please contact Mary Beth Sheffield at (850) 412-3978.

Sincerely,

Elizabeth Dudek
Interim Secretary

ED/mbs
Enclosure: Response to the Preliminary and Tentative Information Technology Audit of FMMIS and DSS
cc: Roberta Bradford, Director of Medicaid
Alan Strowd, Bureau Chief of Medicaid Contract Management

2727 Mahan Drive • Mail Stop #1
Tallahassee, FL 32308

Visit AHCA online at AHCA.MyFlorida.com

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

FLORIDA MEDICAID
A Division of the Agency for Health Care Administration
Better Health Care for all Floridians

CHARLIE CRIST
GOVERNOR

ELIZABETH DUDEK
INTERIM SECRETARY

Agency for Health Care Administration
Response to the Auditor General's preliminary and tentative findings regarding the Information Technology Operational Audit report dated October 20, 2010. This audit specifically addressed the Florida Medicaid Management Information System (FMMIS) and the Decision Support System (DSS) for the period of July 1, 2009 through June 30, 2010, and selected Agency actions through September 28, 2010.

Finding Number 1: Access Control Documentation
The Agency, together with HP, should improve its procedures for user account management by maintaining adequate documentation of the authorizations and business justifications for the assignment of user access privileges.

AHCA Response: The Agency acknowledges the finding. As a result of these findings the Security Request form is being revised with more user friendly Position to Roles documentation for the servers and database access. These changes will mirror the documentation that has since been put into place and that is currently in use for the FMMIS applications process. HP will complete the documentation enhancement with approval of Medicaid Contract Management by November 30, 2010.

Finding Number 2: Appropriateness of Access Privileges
The Agency and HP should review, and adjust as appropriate, the access privileges described in 'Finding Number 2' to limit access privileges to only what is needed to perform job responsibilities.

AHCA Response: The Agency acknowledges the finding. HP will audit the entire Florida account for database, server, change control management and FMMIS/DSS application access for appropriateness of roles. All security request forms will be updated to reflect the appropriate access for all users. The audit and updated forms will be completed by December 31, 2010.

Finding Number 3: Timely Disabling of Access Privileges
The Agency should work with HP to ensure that the access privileges of former contractors are timely disabled to minimize the risk that data and IT resources could be misused by the former contractors or others.

AHCA Response: The Agency acknowledges the finding. NACO's (Network Application Control Online System) controls all areas of access. There is an existing SLA (Service Level Agreement) requirement to ensure that all ID's are terminated within four hours. To ensure they

2727 Mahan Drive • Mail Stop #1
Tallahassee, FL 32308

Visit AHCA online at AHCA.MyFlorida.com

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

meet this SLA requirement, HP is updating procedures to provide clear direction on actions to be taken whenever contractors transfer to another HP account or another role within the Florida account. The updated procedures document will be completed and approved by Medicaid Contract Management (MCM) by November 30, 2010. All contractor access privileges were reviewed and updated in August 2010.

Finding Number 4: Access Control Records Retention
The Agency should ensure that access control records are retained as required by the General Records Schedule.

AHCA Response: The Agency acknowledges the finding. The loss of records was due to individuals inadvertently deleting accounts instead of inactivating accounts. HP will clarify procedures and provide training to all individuals that participant in the activation/deactivation of accounts function. This will be completed by November 30, 2010.

Finding Number 5: Periodic Review of Access Privileges
The Agency should ensure that periodic reviews are conducted of the ongoing appropriateness of access privileges for the FMMIS and DSS applications, server operating systems, databases, and program change management software to facilitate the timely detection and correction of excessive or unnecessary capabilities.

AHCA Response: The Agency acknowledges the finding. The Agency has a copy of the fiscal agent's schedule for the review of access privileges regarding the FMMIS and DSS applications, server operating systems, databases, and program change management software. The Agency will review and conduct periodic, unannounced audits to ensure the fiscal agent is performing reviews and taking appropriate action.

Finding Number 6: User Identification
The Agency should require HP to assign unique user IDs to all individual users authorized to perform database administration functions for FMMIS and DSS.

AHCA Response: HP has changed the operational use associated to the IDs and has conducted training to educate the users. These IDs have been included in the ongoing audit procedures to ensure the usage is appropriate, the Agency understands there are currently 17 individuals that have access to these IDs. These individuals make up a core HP team of "floaters," who are assigned to various state accounts on temporary bases to assist with additional or "expert" coding and testing. The Agency has approved this current process. While contractor individuals may not be specifically identifiable by log-in information, AHCA will discuss with the contractor alternative tracking and review processes to identify the specific users.

Finding Number 7: Other Security Controls
The Agency should implement appropriate security controls in the areas of user authentication, session controls, and logging of system activity to ensure the continued confidentiality, integrity, and availability of Agency data and IT resources.

AHCA Response: The Agency implemented several of the suggested recommendations of the audit inquiry that was concluded October 2009. These changes were implemented in Mid April 2010. Medicaid Contract Management has prepared a separate response for internal records.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Finding Number 8: Program Change Controls
The Agency, with the assistance of HP as applicable, should accurately document and enforce effective program change controls that provide for appropriate authorization, timely testing, and approval of changes. Additionally, to ensure that only authorized and properly functioning changes are made to FMMIS and DSS and implemented in a consistent manner pursuant to management's expectations, the Agency should log and review program changes that are moved into the production environment.

AHCA Response: The Agency will review the Change Control Procedures updating any areas that are not reflective of current change control policy or may not be adequate to ensure proper control authorization and accuracy. The fiscal agent will create a new weekly report of all implemented coding changes. This new report will be compared to the comparable week's promotion to ensure that only those changes approved by the State were promoted (exception for cycle monitor changes) and to ensure that all intended changes were promoted. Medicaid Contract Management will be copied on the results of the review. The change control procedure's review and new audit reporting will be completed by January 31, 2011.

Finding Number 9: Prioritizing Customer Service Requests
The Agency should ensure that CSRs are adequately researched and prioritized to ensure that recipient eligibility processing errors are resolved in a timely manner.

AHCA Response: The Agency is committed to ensuring that Medicaid benefits are paid only on behalf of eligible recipients. The Agency will ensure that future recipient eligibility processing errors are adequately researched (including any impact to dollars or claim counts or caseload), effectively prioritized in a CSR and timely resolved.

Finding Number 10: Claims Resolution Quality Reviews
The Agency should ensure that HP reinstates its claims resolution quality control reviews to provide assurance that claims subject to manual resolution are processed accurately and correctly by the Resolutions Department.

AHCA Response: The Agency acknowledges the finding. On October 27, 2010, Medicaid Contract Management instructed HP through MCM letter 64492-10 to reinstate this procedure immediately as well as requiring HP to supply the report and back-up documentation as part of the SLA report card. This report is to be supplied to Contract Management on the first of every month for the prior month's QC activity.