Thomas A. Schweich

Missouri State Auditor

SOCIAL SERVICES

Medicaid Management Information System Data Security

March 2013

Report No. 2013-020

http://auditor.mo.gov

Thomas A. Schweich
Missouri State Auditor

CITIZENS SUMMARY

Findings in the audit of the Department of Social Services, Medicaid Management Information System Data Security

Background	The Medicaid Program provides health care access to low-income persons age 65 or over, blind, disabled, members of families with dependent children, children and pregnant women in poverty, refugees, and children in state care. The Medicaid Management Information System (MMIS) is the Medicaid benefit claims processing and information retrieval system used by the state to meet requirements of the United States Department of Health and Human Services. The MMIS is owned by the state but is operated and maintained by a contracted vendor. During processing, claims are subject to numerous "edit checks" (also known as data validity checks), which is program code that tests input for correct and reasonable conditions. Medicaid claims paid in calendar year 2011 totaled over $6.6 billion. The scope of our audit included security controls and other relevant internal controls established and managed by the Department of Social Services (DSS), MO HealthNet Division (MHD).
Claims Processing	The MHD paid claims of over $62,400 during calendar year 2011 for services that should not have been allowed because three edit checks were not functioning properly. The MHD does not routinely review edits to ensure the testing criteria remain accurate, so management does not have the necessary assurance that edits are working properly and only claims meeting program guidance are paid. An authorized user may override a denied claim, but the MHD cannot always track the identity of users who performed an override, which reduces accountability. The MHD did not always ensure edit documentation was complete and accurate. Audit staff found four active edits for organizations that no longer had a managed care contract with MHD, one edit that was disabled, and several instances where the criteria in the edit documentation lacked some relevant data fields.
User Account Controls	DSS management and the MMIS contractor have not established or documented adequate user account management policies and procedures. DSS management could not identify the user of an account with privileged access to the MMIS. Failing to identify all users with privileged access to the MMIS could leave the system at risk of improper modification. DSS management has not implemented sufficient procedures for periodically reviewing user access rights to the MMIS to ensure access rights remain appropriate. Audit staff found 66 active user accounts for individuals who had terminated employment from the DSS or one of the contractors. In addition, multiple users were assigned to the same internal MMIS identifier accounts, making it difficult to identify users responsible for making changes to the MMIS. The DSS has not established procedures to prevent a single user from accessing the MMIS from more than one location at any given time. Such concurrent session controls help protect the confidentiality, integrity, and availability of the data and the system.

MMIS Contract	The DSS has not performed a comprehensive security control risk assessment for the MMIS, which is a responsibility inherent to the owners of a system. Neither the DSS nor the contractor has documented the minimum levels of output, such as the number of claims processed in a period of time, or system availability expected from the MMIS, so neither party can ensure the system is operating at acceptable levels. Moreover, the DSS has not ensured the MMIS contractor is in full compliance with contractual requirements. For example, the MMIS contractor has not provided documentation to the DSS of key disaster recovery procedures, as required by the contract.

In the areas audited, the overall performance of this entity was **Fair**.*

American Recovery and Reinvestment Act (Federal Stimulus)	Not applicable.

*****The rating(s) cover only audited areas and do not reflect an opinion on the overall operation of the entity. Within that context, the rating scale indicates the following:

Excellent: The audit results indicate this entity is very well managed. The report contains no findings. In addition, if applicable, prior recommendations have been implemented.

Good: The audit results indicate this entity is well managed. The report contains few findings, and the entity has indicated most or all recommendations have already been, or will be, implemented. In addition, if applicable, many of the prior recommendations have been implemented.

Fair: The audit results indicate this entity needs to improve operations in several areas. The report contains several findings, or one or more findings that require management's immediate attention, and/or the entity has indicated several recommendations will not be implemented. In addition, if applicable, several prior recommendations have not been implemented.

Poor: The audit results indicate this entity needs to significantly improve operations. The report contains numerous findings that require management's immediate attention, and/or the entity has indicated most recommendations will not be implemented. In addition, if applicable, most prior recommendations have not been implemented.

Department of Social Services
Medicaid Management Information System Data Security
Table of Contents

THOMAS A. SCHWEICH
Missouri State Auditor

Honorable Jeremiah W. (Jay) Nixon, Governor
and
Alan O. Freeman, Director
Department of Social Services
and
Dr. Ian McCaslin, Director
MO HealthNet Division
Jefferson City, Missouri

We have audited the Department of Social Services, MO HealthNet Division controls related to the Medicaid Management Information System (MMIS) in fulfillment of our duties under Chapter 29, RSMo. This audit was conducted to evaluate the effectiveness of security controls and other related internal controls designed to secure confidential citizen information and health-related data, and because the MMIS processes over $6 billion of state and federal expenditures each fiscal year. The objectives of our audit were to:

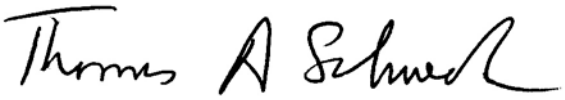
1. Evaluate the security controls and other related internal controls designed to ensure the confidentiality, integrity, and availability of data and information processed and maintained by the MMIS.

2. Evaluate the economy and efficiency of certain management practices and information system control activities.

3. Evaluate compliance with certain legal provisions including certain provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules.

We conducted our audit in accordance with the standards applicable to performance audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform our 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 such a basis.

For the areas audited, we identified (1) deficiencies in security and related internal controls, (2) the need for improvement in management practices and procedures, and (3) no significant noncompliance with legal provisions. The accompanying Management Advisory Report presents our findings arising from our audit of the Department of Social Services, MO HealthNet Division, Medicaid Management Information System.



Thomas A. Schweich
State Auditor

The following auditors participated in the preparation of this report:

Deputy State Auditor:	Harry J. Otto, CPA
Director of Audits:	John Luetkemeyer, CPA
Audit Manager:	Jeffrey Thelen, CPA, CISA
In-Charge Auditor:	Lori Melton, M.Acct., CPA
Audit Staff:	Patrick M. Pullins, M.Acct., CISA
	Erica Schroer

Department of Social Services
Medicaid Management Information System Data Security
Introduction

Background

Data security is a critical consideration for any organization dependent on information systems and networks to meet its mission or business objectives. Data security is especially important for state agencies, where public trust is essential for the efficient delivery of services. Security can be a significant investment, which adds to an already long list of administrative duties. Managing secure networks, developing and implementing new system functionality, maintaining system users, and other day-to-day security tasks can strain limited administrative resources. However, agency management must understand proper protection of citizen information is a requirement and not a luxury in the current interconnected cyber environment. Without proper safeguards and controls, computer systems and confidential data are vulnerable to individuals with malicious intentions who can use access to obtain sensitive data or disrupt operations.

The Medicaid Program, authorized by federal legislation in 1965, provides health care access to low-income persons age 65 or over, blind, disabled, or members of families with dependent children. Legislative changes have expanded the categories of eligibility to include Medicaid coverage for children and pregnant women in poverty, refugees, and children in state care. The Missouri Medicaid program is administered by the state and is jointly financed by the federal and state governments. The Department of Social Services (DSS), MO HealthNet Division (MHD), is responsible for administration of the Medicaid program.

The Medicaid Management Information System (MMIS) is the Medicaid benefit claims processing and information retrieval system used by the state to meet the requirements of the United States Department of Health and Human Services. The system was established in the 1980s and replaced by an enhanced system in 2009. The MMIS has also been subject to continuous updates to account for changes in program rules and regulations. The MMIS is owned by the state[1] but is operated and maintained by a contracted vendor. The contractor, who has physical possession of the system, is responsible for certain operational aspects, including processing claims and system maintenance. The MHD MMIS unit is responsible for monitoring contractor performance, as well as other administrative and operational aspects of the system.

According to accepted standards, security controls are the management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. Confidentiality refers to preserving

[1] A system owner's responsibilities include providing for appropriate security and establishing controls to ensure the confidentiality, integrity, and availability of the system and data.

authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information. Integrity relates to guarding against improper information modification or destruction, and availability ensures timely and reliable access to and use of information.

Claims Processing

Medicaid providers submit claims to bill the state for medical services provided to Medicaid participants. Most claims are submitted electronically, however, some claims are submitted on paper. All submitted claims are entered in and processed by the MMIS to determine the allowable amount paid for each claim.

During processing, claims are subjected to numerous edit[2] checks. These edits perform tests to ensure claims are reasonable and appropriate, and meet program guidance before allowing claims to be paid. For example, edits are used to ensure:

- Claims are submitted with the name and identification number of an authorized Medicaid participant.
- Claims are submitted within a year of the date of service.
- Claims are not paid more than once.

Certain edits do not prevent claims from being processed and paid, but instead flag claims for further review. Other edits require claims to be corrected or reviewed by program staff to determine if an edit override action should be applied to force a claim to process.

Many edits are controlled by criteria coded in specific reference tables in the MMIS. These tables allow program staff to more easily modify the specific criteria an edit is testing against.

Scope and Methodology

The scope of our audit included security controls and other related internal controls established and managed by the MHD; policies and procedures; and other management functions and compliance issues in place during the 2 years ended June 30, 2012.

Our methodology included conducting interviews with appropriate officials and staff; obtaining and reviewing available policies and procedures, federal laws, and other applicable information; and performing testing.

[2] An edit, also known as a data validity check, is program code that tests the input for correct and reasonable conditions; such as account numbers falling within a range; numeric data being all digits; dates having a valid day, month, and year; etc.

We obtained user account data from the MHD and the system contractor as of March 2012. To ensure completeness of the data, we reviewed user accounts for reasonableness and scanned the names of employees. Although we used computer-processed data from MHD systems to identify user accounts and related information, we did not rely on the results of any processes performed by these systems in arriving at our conclusions. Our conclusions were based on our review of the controls over user accounts.

We obtained the employment records of all DSS employees for fiscal years 2001 to 2012 from the statewide accounting system for human resources. We matched these records to user accounts with access to the MMIS system to determine if any terminated employees had active user accounts. We provided DSS officials a list of all terminated employees we found who had active access to the MMIS system. Although we used computer-processed data from the human resources system for our audit work, we did not rely on the results of any processes performed by this system in arriving at our conclusions. Our conclusions were based on our review of the issues specific to the audit objectives.

We obtained data from the MMIS system for all claims paid or denied during calendar year 2011. The claims paid in calendar year 2011 totaled over $6.6 billion. To ensure completeness of the data, we performed basic reasonableness tests, reviewed claim types, and reconciled the paid amounts from the data file to control totals from the system. Although we used computer-processed data from the MMIS for our audit work, we did not rely on the results of any processes performed by this system in arriving at our conclusions. Our conclusions were based on our review of the issues specific to the audit objectives.

To determine whether controls to validate and edit MMIS claim records were in operation and working effectively, we reviewed MMIS and provider manuals, reviewed system documentation, and interviewed MHD staff. We analyzed claim records for compliance with certain system edits to ensure existing edits were functioning properly. We provided MHD officials with a list of overpayments and potential overpayments identified in the audit.

We based our evaluation on accepted state, federal, and international standards and best practices related to information technology security controls from the following sources:

- National Institute of Standards and Technology (NIST)
- Government Accountability Office (GAO)
- ISACA (formerly known as the Information Systems Audit and Control Association)

1. Claims Processing

Department of Social Services (DSS), MO Healthnet Division (MHD) management did not ensure all claims were processed accurately. Errors in edit testing criteria used by the Medicaid Management Information System (MMIS) to process claims resulted in payments of over $62,400 for claims that should have been denied and not paid during calendar year 2011. In addition, deficiencies in recording user information in claim records for certain edit overrides and incomplete edit documentation reduced the effectiveness of security and related internal controls.

1.1 Improper Payments

The MHD paid claims of over $62,400 during calendar year 2011 for services that should not have been allowed. These claims were processed and paid because three edit checks were not properly functioning.

We tested two edits designed to detect instances of monthly services being billed more than once in a month or daily services being billed after claims had already been billed on a monthly services basis. In 2011, the MMIS processed $2.2 million in paid claims that should have been subject to these two edits. We found the edits failed to detect multiple monthly billings in a single month, which allowed over $61,100 of improper payments. We also found the edits did not detect instances of daily claims after a monthly claim had already been submitted, which allowed over $900 of improper payments. These improper payments occurred because certain edit criteria used by the MMIS to process claims was inaccurately specified from 2009 through August 2012, when we brought the issue to the attention of MHD management.

We also tested an edit designed to prevent payments to providers for performing both a consultation and specific services to the same participant on the same date, a practice that is not allowed by federal regulations. The MMIS processed $45.2 million in paid claims during 2011 that met the criteria to be tested by this edit. While the edit appeared to function properly on the vast majority of claims, we identified approximately $400 of improper payments made to providers that billed for both services and consultation on the same date. MHD staff could not identify why the edit did not detect these claims.

Additionally, we found a fourth edit check failed to function properly, resulting in two claims being processed with the same claim number. In this instance, neither claim resulted in an actual payment since the two duplicated claims were adjustment claims to reverse previously approved claims.

MHD management does not routinely review edits to ensure the testing criteria remains accurate. Reviews are only performed when problems are identified or other changes are necessary, according to MHD management. As a result, the MHD does not have necessary assurance that edits are

working properly and only claims meeting program guidance are paid. Implementing procedures to periodically review edits for accuracy and completeness would help prevent payment of improper claims and would lead to detection of errors in a more timely manner.

1.2 Override Audit Records

The MHD cannot always track the identity of users who performed an override of a claim denied by an established edit. A denied claim may be overridden by authorized users and subsequently paid for a variety of reasons. Information to identify the user account that applied the override is posted on the claim to provide an audit record of the override. However, we found that for two edits, in certain circumstances, default user account information is posted to the claim record rather than the actual account information of the user applying the override. As a result, if an unauthorized override was applied, the MHD would not be able to readily determine which user applied the override to the claim.

Accepted standards require information systems to produce audit records that contain sufficient information to, at a minimum, establish what type of event occurred and the identity of any user/subject associated with the event. Without recording the identity of the user account that performed the override, accountability for the override is lacking.

1.3 Edit Documentation

The MHD did not always ensure edit documentation was complete and accurate. We found several instances where edit documentation did not match the actual criteria or edit coding and instances where edits had been disabled but the documentation not updated to indicate the control was no longer functioning. As a result, it becomes increasingly difficult for the MHD to administer edit controls and ensure edits are functioning properly to prevent payments that are not appropriate and do not meet program guidance.

Expired Contracts

Managed care organizations, not the Medicaid program, are responsible for medical costs for participants enrolled in managed care. As a result, separate edits for each organization have been established to deny claims for participants enrolled with a managed care program. We found four active edits for organizations that no longer had a managed care contract with the MHD. Edits for two of the four managed care organizations were still in place over 13 years after the contracts had been terminated while the remaining two edits were still active over 5 years after the contracts had been terminated. Without a current contract, Medicaid participants are not enrolled with these organizations and the edits are no longer necessary.

Edits turned off

Claims submitted to adjust a previous claim should reference the same participant as the original claim, according to system documentation. We found approximately 1,300 adjustments, processed in calendar year 2011, that referenced a different participant on the adjustment claim than the

original claim. After research, MHD program staff said this edit was no longer used. However, the edit documentation had not been updated to indicate the status and did not contain authorization for disabling the control.

Insufficient details

We found instances where the criteria described in the edit documentation did not include some relevant data fields. Several edits were designed to limit access to certain services within a period of time. However, most of these edits did not describe actual testing criteria or document that limits are specific to a single provider.

For example, claims submitted to the MMIS include two categories of providers. The "Provider" on the claim is generally used to indicate where the participant received services, such as a hospital, clinic, or practice. The "Performing Provider" is used to record the specific staff member who performed the services being billed, such as a doctor or nurse. We reviewed several edits where the documentation did not specify the category of provider to be tested. MHD staff agreed the documentation did not specifically describe the actual testing performed by the edit. Instead, the MHD relied on documentation in the programming code because the edit testing was difficult to describe.

A key element of information security is to test and evaluate policies, procedures, and controls to determine whether they are current, effective, and operating as intended. Without accurate and complete edit descriptions, management cannot ensure the controls are interpreted correctly by staff to identify and mitigate areas of control risk and noncompliance with program guidelines.

Recommendations

The DSS:

1.1 Ensure all edit criteria specified in claim processing reference tables are complete and accurate. In addition, the DSS should identify and recoup any overpayments made to providers due to inaccurate edits.

1.2 Ensure the user account that applied an exception override is recorded in all cases.

1.3 Ensure edit documentation is complete, accurate, and properly reflects actual testing procedures performed during claims processing.

Auditee's Response

1.1 DSS will review the identified claims and recoup any claims paid in error. Edit documentation is reviewed and updated as needed when exceptions are researched or modified. Staff researching or monitoring claims processing edits have access to the rules engine

that houses the detailed edit criteria used in claims processing. Future enhancements will eventually move the remaining edits into the rules engine providing staff with access to exception post criteria details. The exception control file houses a description of the edit; however, the detailed criteria used to process claims is housed in the rules engine, hard coding, and/or system parameters. The purpose of the exception control file is to provide a high level description of the edit and the edit status that will post to the claim (suspend, deny, report).

1.2 DSS has initiated a system request to ensure user account information is recorded on Exception overrides.

1.3 Edit documentation is reviewed and updated as needed when exceptions are researched or modified. Staff researching or monitoring claims processing edits have access to the rules engine that houses the detailed edit criteria used in claims processing. Future enhancements will eventually move the remaining edits into the rules engine providing staff with access to exception post criteria details. The exception control file houses a description of the edit; however, the detailed criteria used to process claims is housed in the rules engine, hard coding, and/or system parameters. The purpose of the exception control file is to provide a high level description of the edit and the edit status that will post to the claim (suspend, deny, report).

2. User Account Controls

DSS management and the MMIS contractor have not established or documented adequate user account management policies and procedures. User account management includes requesting, establishing, issuing, suspending, modifying, closing, and periodically reviewing user accounts and related user privileges, according to accepted standards. User account management policies and procedures should be established for all user accounts, including system administrators and other privileged users.

2.1 Unidentified Privileged Account

DSS management could not identify the user of an account with privileged access to the MMIS.

Privileged users are individuals who have access to system control, monitoring, or administration functions (such as a system administrator). According to accepted standards, privileged access should be limited to only those individuals who need the functions to perform their job duties due to their significant access rights, and should be monitored to ensure actions performed are in accordance with the user's business requirements.

We reviewed user records for all staff with access to the MMIS to determine which users had privileged account access. For the users with privileged

access, we matched the user account to employee records from the state human resources system or to a listing of contractor employees. We found one user account, identified as a "Test Clerk" in the user account list, that could not be matched to either the state or contractor employee listings. DSS staff could not identify the specific individual to whom this account was assigned, and believe the account may have been shared by system programming staff. This account had been used to change system security settings, according to system audit logs. Documentation approving this change was available; however, the change should not have been performed by an unidentified user.

Failing to positively identify all users with privileged access to the MMIS could leave the system at risk of improper modification. Further, by allowing shared accounts to be used, any improper modifications cannot be associated with the individual(s) responsible. In addition, the Health Insurance Portability and Accountability Act requires employees to have only appropriate access to Protected Health Information (PHI), including preventing employees without a need to access PHI from obtaining such access.[3]

2.2 Management review of user accounts

DSS management has not implemented sufficient procedures for periodically reviewing user access rights to the MMIS to ensure access rights remain appropriate. Both DSS and contractor security policies require reviews of user access to information systems periodically or when user access requirements change. Accepted standards also support regular review of all accounts and related privileges.

Terminated employees

The MHD did not always ensure MMIS access was removed timely when the user was no longer employed in a position needing access. Of the 878 active user accounts as of March 2012, we found 66 accounts for individuals who had terminated employment from the DSS or one of the contractors. In 58 of these instances, account access was not removed because MMIS system administrators were not informed these employees had terminated employment. In eight of these instances, the MHD did remove access but not until at least 30 days after the user was no longer employed.

By allowing accounts belonging to terminated users to exist in the MMIS, management may increase the risk of unauthorized access and compromise the confidentiality and integrity of data maintained by the DSS.

System access

Management has not regularly reviewed user accounts to ensure access rights are appropriate and remain aligned with current job duties.

[3] HIPAA Security Rule, 45 CFR 164.308

Periodically reviewing user accounts could have identified the following problems we found:

- One user was issued two accounts (one under a misspelled name). The error was not detected because the user marked both access request forms as if the account was for a new user.
- Four users with read access to system security tables. These users previously required access, but a reassignment of responsibilities meant access to security tables was no longer necessary to perform job duties. Access to the security tables was removed when we brought the issue to management's attention.
- Thirteen users with inappropriate access to the provider master files. Eight users were MMIS contractor staff, two users were employed by subcontractors, and the remaining three users were MHD employees. Based on our request to review these user accounts, MHD management determined these users did not need the level of access to provider master files they had been granted.
- Six user accounts created for individuals who transferred to different divisions without deleting the previous account, allowing these users to have two accounts simultaneously.

Without periodically reviewing user access rights, management faces an increased risk that unauthorized alterations of the rights will go undetected or access rights may not be aligned with current job duties.

Shared accounts

Multiple users were assigned to the same internal MMIS identifier accounts. However, MHD management did not regularly review these accounts to ensure access granted was appropriate.

Access rights are assigned to user accounts. However, the MMIS uses internal identifiers, which are separate from user accounts, to log actions performed by users. Because the MMIS has a limited number of these identifiers available, multiple user accounts are often assigned to the same identifier. The practice of sharing identifiers has the potential to limit accountability of changes made in the system. To alleviate this concern, the DSS has attempted to ensure, at any point in time, only one user is assigned an identifier with authority to update information. However, without reviewing the accounts periodically, management cannot ensure only one of the users sharing the account has access to update information.

Accepted standards, including DSS policy, require all users to have uniquely identifiable user accounts. Allowing multiple users to share the same account makes it difficult, if not impossible, to identify the user responsible for making changes to the MMIS.

2.3 Concurrent Sessions

The DSS has not established procedures for the MMIS to limit the maximum number of concurrent sessions for each user. Concurrent session controls prevent a single user from accessing an information system from more than a specified number of locations at any given time. This control helps prevent unauthorized users from accessing the system by masquerading as an authorized user.

DSS management said multiple sessions are necessary because users often need to view multiple screens at once on a single desktop. MMIS contractor staff said a system control locks an account after 2 hours of inactivity to limit unauthorized access. However, the inactivity control does not prevent users from accessing the MMIS at another location, such as a second computer. While both controls help prevent unauthorized access, inactivity controls work when an access point is left unattended, whereas concurrent session controls prevent an unauthorized user from accessing the system at the same time an authorized user is logged in from a different location.

According to accepted standards, the number of concurrent sessions for a user should be limited. Without limiting access from multiple locations at the same time, management may not be able to ensure the confidentiality, integrity, and availability of data and the system.

Recommendations

The DSS:

2.1 Ensure all MMIS access can be associated with specific users and access rights granted to each user are appropriate for their job duties.

2.2 Ensure all user access to the MMIS is periodically reviewed by management and inappropriate access, including that of terminated users, is removed in a timely manner.

2.3 Establish security settings limiting the number of concurrent sessions for a single user.

Auditee's Response

2.1 DSS established a dedicated Privacy and Security Officer position in April 2012 to address the security management needs specific to the MO HealthNet Division. Reviews of MMIS access will continue to be performed at the time the request is received; periodic reviews will occur to verify user access rights are appropriate and still required.

2.2 DSS established a dedicated Privacy and Security Officer position in April 2012 to address the security management needs specific to the MO HealthNet Division. Periodic reviews will occur to verify

user access rights are appropriate and to ensure timely removal of access from the MMIS.

2.3 It is important for the workflow of the DSS to maintain multiple sessions. The DSS is working with the fiscal agent to identify options for limiting sessions while maintaining workflow.

3. MMIS Contract

DSS management has not ensured the MMIS contract is fully complied with and includes some necessary provisions to ensure the confidentiality, integrity, and availability of the system and related data. This has occurred because the DSS has not performed a comprehensive risk assessment, defined acceptable levels of output of the system, or ensured the contractor is in compliance with the contract.

3.1 Security Risk Control Assessment

The DSS has not performed a comprehensive security control risk assessment for the MMIS.

The MMIS contract requires the contractor to perform a periodic comprehensive security risk analysis for the MMIS, which DSS management said is performed biannually. In addition, the DSS performs limited security risk analysis when reviewing planned changes to the MMIS. However, these DSS reviews are limited in scope to only the planned changes and do not review how changes could have unintended consequences in other functions of the system.

A security risk assessment is a responsibility inherent to the owners of a system. Accepted standards require owners to make decisions about classifying information and systems and protecting them in line with this classification. Standards also emphasize the risk management process should not be treated primarily as a technical function carried out by the technology experts who operate and manage the system, but as an essential management function of the organization. By outsourcing risk assessment to the contractor, the DSS has abdicated a key ownership responsibility and cannot ensure the controls in place are adequate to protect the confidentiality, integrity, and availability of the data within the MMIS.

3.2 Minimum Levels of Output

Neither the DSS nor the contractor has documented the minimum levels of output, such as the number of claims processed in a period of time, or system availability expected from the MMIS. As a result, neither party can ensure the system is operating at acceptable levels, or begin remediation efforts should the operation drop below acceptable levels.

The MMIS contract requires the contractor to create a Business Continuity Plan for the MMIS. According to the contract, the Business Continuity Plan "must identify potential system failures" and "contain a risk analysis for each core business process." The contract also requires the contractor to

define the minimum acceptable level of output for each core business process. The contractor has created a Business Continuity Plan, which includes a list of core business processes, but the minimum level of output for each core business process has not been documented.

By not documenting the level of output expected from the system, DSS management cannot ensure the system is operating effectively.

3.3 Contract Monitoring

The DSS has not ensured the MMIS contractor is in full compliance with contractual requirements. For example, the MMIS contract includes extensive requirements related to the provision of disaster recovery services for the MMIS. The contractor has not provided documentation to the DSS to support compliance with these disaster recovery requirements.[4]

Failure to document key disaster recovery procedures subjects the MMIS to risks that the system may not be readily restored in the event of a disaster, causing the MMIS to be non-operational for an extended period of time. Without ensuring compliance with all contractual requirements, the DSS cannot ensure the contractor has taken steps to minimize the risk to the MMIS in the event of a disaster.

Recommendations

The DSS:

3.1 Ensure risk assessments, including security control analyses, are completed for the MMIS and reviewed in a timely manner.

3.2 Work with the MMIS contractor to ensure minimum acceptable levels of system output are determined and documented to provide measured baseline levels of service expected from the MMIS.

3.3 Require the MMIS contractor to document and demonstrate compliance with contract requirements, including the provisions for disaster recovery services.

Auditee's Response

3.1 DSS agrees with this recommendation.

3.2 DSS has established system expectations to return to normal operations within 72 (seventy-two) hours, which are covered in the fiscal agent Business Continuity, Contingency and Disaster Recovery plan.

[4] We provided DSS management a list of the critical services included in the contract for which documentation of compliance could not be provided.

3.3 DSS will continue to work with the fiscal agent to monitor and improve the Disaster Recovery and Backup Plan as required in Section 9.1.28 of the contract. The State has requested, through the Budget process, additional dedicated staff to monitor MMIS contract compliance.