



**Auditor of State
Betty Montgomery**

TABLE OF CONTENTS

I	INDEPENDENT ACCOUNTANT’S REPORT	1
II	ORGANIZATION’S DESCRIPTION OF CONTROLS	
	CONTROL OBJECTIVES AND RELATED CONTROLS	3
	ORGANIZATION	3
	RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING	4
	Control Environment.....	4
	Risk Assessment.....	5
	Monitoring.....	5
	INFORMATION AND COMMUNICATION	5
	GENERAL EDP CONTROLS	6
	Overall Operation of the IT Function	6
	Development and Implementation of New Applications and Systems	7
	Changes to Existing Applications or Hardware Systems	7
	IT Security	10
	IT Operations.....	12
	APPLICATION CONTROLS.....	14
	Multi-Agency Community Services Information Systems (MACSIS).....	14
	USER CONTROL CONSIDERATIONS	19
III	INFORMATION PROVIDED BY THE SERVICE AUDITOR	
	GENERAL EDP CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS	22
	Overall Operation of the IT Function	22
	Changes to Existing Applications or Hardware Systems	24
	IT Security	27
	IT Operations.....	31
	APPLICATION CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS	33
	Multi-Agency Community Services Information Systems (MACSIS).....	33

This Page Intentionally Left Blank



Auditor of State Betty Montgomery

INDEPENDENT ACCOUNTANT'S REPORT

ODMH / ODADAS
Multi-Agency Community Services Information Systems (MACSIS)
State Office Tower, Floor 11
Columbus, Ohio 43215

To the Ohio Department of Mental Health and the Ohio Department of Alcohol and Drug Addiction Services:

We have examined the accompanying description of controls of the Ohio Department of Mental Health (ODMH) and the Ohio Department of Alcohol and Drug Addiction Services (ODADAS) applicable to the processing of transactions for users of the Multi-Agency Community Services Information Systems (MACSIS). Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of the ODMH's and ODADAS's controls that may be relevant to a user board's internal control as it relates to an audit of financial statements; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily and user boards applied the internal controls contemplated in the design of the ODMH's and ODADAS's controls; and (3) such controls had been placed in operation as of December 31, 2004. The department's servers which process the MACSIS application and certain firewall equipment are physically located in the computer rooms at the State Office Tower (SOT) and the State of Ohio Computer Center (SOCC). The accompanying description includes only those controls and related control objectives of the ODMH and ODADAS and did not include controls and related control objectives of the SOT and SOCC. Our examination did not extend to controls at the SOT and the SOCC. The control objectives were specified by the management of the ODMH and ODADAS for MACSIS. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

As discussed in the accompanying description, minimum password length and password expiration parameters do not meet established standards, and sign-on parameters have not been established to prevent a high number of failed logon attempts to the Diamond 725 component of MACSIS. The deficiency resulted in procedures not being suitably designed to meet the control objective, "Access to particular functions within applications (e.g., approving payment of vendors) should be appropriately restricted to ensure the segregation of duties and prevent unauthorized activity."

In our opinion, the accompanying description of the aforementioned applications presents fairly, in all material respects, the relevant aspects of the ODMH's and ODADAS's controls that had been placed in operation as of December 31, 2004. Also, in our opinion, except for the matter described in the preceding paragraph, the controls, as described, are suitably designed to provide reasonable assurance the specified control objectives would be achieved if the described controls were complied with satisfactorily and user boards applied the controls contemplated in the design of the ODMH's and ODADAS's controls.

In addition to the procedures we considered necessary to render our opinion as expressed in the previous paragraph, we applied tests to specific controls, listed in Section III, to obtain evidence about their effectiveness in meeting the control objectives, described in Section III, during the period from January 1, 2004 to December 31, 2004. The specific controls and the nature, timing, extent, and results of the tests are listed in Section III. This information has been provided to user boards of the ODMH and ODADAS and to their auditors to be taken into consideration along with information about the internal control at user boards, when making assessments of control risk for user boards. In our opinion, the controls that were tested, as described in Section III, were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance the control objectives specified in Section III were achieved during the period from January 1, 2004 to December 31, 2004. However we did not test the operating effectiveness of controls designed to achieve the control objective, "Access to particular functions within applications (e.g., approving payment of vendors) should be appropriately restricted to ensure the segregation of duties and prevent unauthorized activity." Accordingly, we express no opinion on the achievement of this control objective.

The relative effectiveness and significance of specific controls at the ODMH and ODADAS and their effect on assessments of control risk at user boards are dependent on their interaction with the controls and other factors present at individual user boards. We have performed no procedures to evaluate the effectiveness of controls at individual user boards.

The description of controls at the ODMH and ODADAS is as of December 31, 2004, and information about tests of the operating effectiveness of specified controls covers the period from January 1, 2004 to December 31, 2004. Any projection of such information to the future is subject to the risk that, because of change, the description may no longer portray the controls in existence. The potential effectiveness of specific controls at the ODMH and ODADAS is subject to inherent limitations and, accordingly, errors or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that (1) changes made to the system or controls, (2) changes in processing requirements, or (3) changes required because of the passage of time may alter the validity of such conclusions.

This report is intended solely for use by the management of the ODMH and ODADAS, its user boards, and the independent auditors of its user boards.



Betty Montgomery
Auditor of State

March 31, 2005

SECTION II - ORGANIZATION'S DESCRIPTION OF CONTROLS

CONTROL OBJECTIVES AND RELATED CONTROLS

The ODMH's and ODADAS's control objectives and related controls are included in section III of this report, "Information Provided by the Service Auditor," to eliminate the redundancy that would result from listing them here in section II and repeating them in section III. Although the control objectives and related controls are included in section III, they are, nevertheless, an integral part of the ODMH's and ODADAS's description of controls.

ORGANIZATION

The Multi-Agency Community Services Information Systems (MACSIS) data processing staff consists of 30 individuals from both the Ohio Department of Mental Health (ODMH) and the Ohio Department of Alcohol and Drug Addiction Services (ODADAS). The primary function of the ODMH and ODADAS is to process and maintain claims information submitted by various providers throughout the state.

ODMH and ODADAS have developed the MACSIS. MACSIS is designed as a central benefits administration system, maintained at the State of Ohio Computer Center (SOCC) and used by community boards and board consortiums across the state.

Community boards have access to the system through a state telecommunications network. The software provides for eligibility checking, enrollment, service assessment, billing, and outcome monitoring functions. The system is HIPAA-compliant and designed to meet all Ohio Department of Job and Family Services (ODJFS), and several federal reporting requirements.

MACSIS is an information system that allows ODMH, ODADAS, and their local boards to manage, measure, and monitor the service utilization of Medicaid, state, and local public funds. Also, MACSIS meets the following objectives:

- Positions the state of Ohio and community boards to support a changing healthcare delivery environment.
- Streamlines and standardizes the flow of information from the community agencies and boards for purposes of claims submission, CMS, and ODJFS reporting requirements.
- Facilitates the determination of client eligibility for publicly-funded behavioral health services.
- Provides the flexibility necessary for a board to operate as a unique line of business and to establish multiple, specific product lines to accomplish business objectives.

There are 57 Alcohol, Drug, and Mental Health, (ADAMH) and community mental health and drug/alcohol boards using MACSIS. Of these 57 boards, some have grouped together to form board consortiums for their county or group of Ohio counties. These boards have contracted approximately 500 providers to perform services for clients enrolled in the MACSIS program. The boards are responsible for the adjudication and payment of behavioral health claims to providers using the state supported MACSIS application. The boards collect all claims from the providers and pre-process them before submitting them to MACSIS to be finalized.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT AND MONITORING

Control Environment

The data processing staff administers, maintains, and controls the MACSIS application. End-user input is received and training is conducted via four main user groups noted below:

- Claims* – Comprises claim processing staff from the local boards and state staff who support the claims process.
- Member* – Comprises enrollment processing staff from the local boards and state staff who support those processes.
- MIS* – Comprises technical support staff from the local boards and the state staff who manage technical issues.
- Finance* – Comprises finance representatives from the local boards and state staff who support the accounts payable process.

These user groups meet on an ad hoc basis to hold training sessions or to discuss changing needs that require modification to MACSIS or related business practices. Minor business practice or system improvements are reported to the Project and Operations Planning (POP) committee. If the suggested improvements are deemed necessary by the POP committee, the requests are forwarded to the MACSIS Operation Management (MOM) committee for implementation.

For major system improvements or business practice issues with a significant impact on the community, issues must be formally raised through the Behavioral Health Operations Committee (BHOC). The purpose of the committee is to resolve operational problems that have statewide implications within the behavioral health system. The BHOC, comprised of board, state, and provider executives, determines if the issue is statewide before proceeding with resolution. A sub-committee of the BHOC, Claims Payment and Operations Committee (CPOC), may assist with issues and make recommendations for resolution.

The IT roles and responsibilities are clearly defined through organizational charts and job descriptions. The organizational charts are updated on an as needed basis by the chiefs of ODMH and ODADAS. ODMH and ODADAS have developed job descriptions which are approved by Department of Administrative Services (DAS) to define and segregate the roles of the MACSIS operation. Board users are responsible for authorization and initiation of all transactions.

Application enhancements and modifications to the MACSIS are initiated in two ways. If the application does not provide a feature or function that ODMH or ODADAS desires, a Program Enhancement form is submitted to the vendor, Perot. Application enhancement requests can also originate from the state and/or county board representatives via the four main user groups (Claims, Member, MIS and Finance).

Additional information regarding the control environment can be found in the section, "Overall Operation of the Information Technology Function" later in section II.

Risk Assessment

The ODMH and ODADAS do not have a formal risk management process. Working in conjunction with the IT initiatives outlined by the state of Ohio's chief information officer (CIO), the deputy state chief information officer, and the administrator of the Office of Statewide IT Policy, the ODMH and ODADAS actively participate in the oversight of their information technological initiatives.

The position of the Office of Information Technology (OIT) CIO provides statewide oversight and leadership for all activities related to information technology including strategic IT planning, data processing, telecommunications, and systems development. The CIO is responsible for optimizing the uses of IT resources, and assuring that the states' investment achieves planned programmatic objectives.

The Office of Statewide IT Policy reviews long-range IT plans for state agencies. These plans outline future IT initiatives and forecasts for upcoming fiscal years. These long-range plans address and are not limited to the following:

- Changes in operating environment.
- New personnel.
- New or revamped information systems.
- Rapid growth.
- New technologies.
- New lines, services or activities.

Monitoring

The ODMH and ODADAS organizations are structured so managers of each department report directly to the respective chiefs. The key management employees for ODMH and ODADAS are experienced with the systems and controls at the ODMH and ODADAS. The ODMH and ODADAS chiefs and supervisory personnel monitor the quality of internal control performance as a routine part of their activities. To assist them in this monitoring, ODMH and ODADAS use a variety of reports to monitor the processes involved in processing transactions for user boards. Hardware, software, the network, computer security, and user help desk reports are continually monitored.

INFORMATION AND COMMUNICATION

The aspects of the information and communication component of internal control as they affect the services provided to user organizations are discussed within the General EDP Controls and Application Controls sections.

GENERAL EDP CONTROLS

Overall Operation of the Information Technology Function

The MACSIS data processing staff consists of 30 individuals from both the ODMH and ODADAS. The breakdown of IT personnel by position is as follows:

ODMH

Data systems administrator (1)
Information technology supervisor (5)
Program analyst (5)
Program specialist (2)
Systems analyst (2)
Data control technician (1)
Data systems scheduler (1)
Network services technician (2)
IT consultant 1 (1)
Management analyst supervisor (1)

ODADAS

Information technology manager (1)
Programmer/analyst (2)
Administrative assistant (2)
Data systems coordinator (3)
Information technology supervisor (1)

ODMH is primarily responsible for operating, maintaining, securing, and administering the MACSIS application. Both ODMH and ODADAS process and maintain claims information submitted by various providers throughout the state relative to each respective agency. In CY 2003, both Departments implemented a parallel MACSIS system implementation strategy for HIPAA. This strategy involved maintaining two separate production environments for pre-July and post-July dates of service. In the fall of 2004, maintenance for the MACSIS pre-HIPAA production environment was discontinued. Claims exceeding 365 days from the date of service were no longer reimbursable; therefore, it was not necessary to continue the parallel system strategy.

ODMH and ODADAS use job descriptions and organizational charts to clearly define the various IT roles and responsibilities. The organizational charts are updated on an as-needed basis by the chiefs of ODMH and ODADAS. Job descriptions, approved by DAS, define and segregate the roles of the MACSIS operation.

ODMH and ODADAS provide training to the IT staff to help ensure the staff has the skills necessary for the complexity of their IT environment. MACSIS staff can also make requests for additional training they believe is necessary to improve their job performance.

ODMH management reviews training for each employee annually during employee evaluations. The ODMH assistant chief is responsible for prioritizing all training for the fiscal year. ODMH's proposed IT training plan is submitted by the ODMH assistant chief, and approved by the ODMH chief. Training documentation is recorded for each course attended by ODMH staff. Online Computer Based Training (CBT) courses are also available through the Internet to all ODMH personnel.

Similarly, ODADAS' proposed IT training plan is submitted by the ODADAS assistant chief, and approved by the ODADAS chief. ODADAS management annually reviews training for each employee during the employee evaluation process. If training is deemed necessary, it is documented as an objective on each applicable employee's evaluation for the following year. Training is recorded and documentation maintained for each course attended by

ODADAS staff.

If additional training is necessary, topics are referred to one of four main user groups (Claims, Member, MIS, and Finance) that meet on an ad hoc basis. Four user group meetings/training sessions were held in CY 2004. State staff also attends weekly MOM meetings for routine information sharing and internal issue discussion.

IT management meets periodically to discuss and oversee the IT function and its related activities. The county board end users' perceptions of the quality of the services provided by the IT function are attained through a defined MACSIS committee structure.

The Office of Information Technology (OIT) requires all state agencies to annually prepare and submit their IT plans to the Office of Statewide IT Policy within OIT for review and coordination of the IT planning process. All agency plans provide their IT information strategies regarding data processing services and acquisition of all information technology hardware and software. ODMH and ODADAS each meet periodically with OIT to discuss updates to their long-range plans. The agencies' plans and the minutes of these meetings are available on the Internet (in PDF format) for public viewing. Each agency's long-range plan provides OIT with data to compile a long-range plan for the entire state of Ohio.

Each plan addresses the overall enterprise, its mission, and key business functions, as well as hardware, software, and personnel issues for the UNIX computing environment. The planners' assessments take into consideration the rapidly changing technology, user demands, and the way state government does business.

Development and Implementation of New Applications and Systems

There were no new applications developed or implemented during calendar year 2004. The MACSIS application was supplied in 1997 from Health Systems Design (HSD), subsequently purchased by Perot Systems in 2000. MACSIS was implemented and fully functioning in 1998.

Changes to Existing Applications or Hardware Systems

MACSIS consists of the following five components:

- Pre-processor programs.
- Diamond 725 system.
- Medicaid eligibility system.
- Medicaid reimbursement process.
- Board financial systems.

ODMH and ODADAS use the Perot Diamond 725 software for the MACSIS claims processing application. The Diamond 725 system includes:

- Membership management.
- Provider contract management.
- Claims adjudication processing.
- Accounts payable.

- Remittance advice.
- Interfaces to Board financial and/or county treasurer systems.

There are 2,183 Diamond 725 programs written in BBx and housed on multiple AIX6000 servers. Source code is copyrighted by Perot Systems.

Diamond 725 v8.3.1d provided a new EDI process, namely Diamond Data Services (DDS) and BeMIS. Although Diamond 725 v8.3.1d was implemented in July 2003 to adhere to HIPAA requirements, the old v5.3x was run in parallel production until July 2004. By the end of calendar year 2003, only 2 percent of claims were being processed through the prior version. Because claims exceeding 365 days from the date of service were no longer reimbursable, maintenance of the MACSIS pre-HIPAA parallel production environment was discontinued in the fall of 2004.

The only upgrade to the Diamond production environment during CY 2004 was the move from version 8.3.1d to version 8.3.1f. Version 8.3.1 f included minor problem fixes and minimal enhancement from the v8.3.1d. The vendor provided four additional releases in CY 2004; however, they were not implemented into the production environment during CY 2004 due to problems noted during acceptance testing.

ODMH/ODADAS maintains a software maintenance agreement with Perot for the MACSIS application residing on the UNIX servers. The agreement allows for maintenance and general and software warranties.

Perot provides release notes to ODMH/ODADAS with each upgrade to give management a description of the changes and to assist them in making informed decisions regarding implementing the upgrades.

There are two ways to initiate program changes to the MACSIS. If ODMH or ODADAS requests a change to the processing, reporting, or functionality, a *program enhancement* must be conducted by Perot. If a change request originates from the state and/or county board representatives relating to an error in the processing or reporting, a *program modification* occurs. These two types of program changes are both conducted in a controlled fashion by Perot.

Program Enhancements

Proposals for major enhancements are initially presented to the MACSIS MOM committee to review budget constraints and project validity. Approval from ODMH/ODADAS program change management is required on all program enhancement forms before submission to the vendor, Perot, for further processing.

Once Perot receives the request, The Perot Program Management Office (PMO) will complete a proposed cost and general design document. The proposed cost and general design document are presented to the MOM committee, the State Leadership, and/or the Behavioral Health Operations Committee for their view on the proposed change. The chiefs approve the final proposal. Original program enhancement forms are logged and maintained by ODMH to monitor the status of all program change projects requested of Perot.

Testing of enhancements is performed in the various areas of Management Information Services (i.e. Claims, Membership, and Accounts Payable) by the MIS Information Technology section supervisors. Each MIS section supervisor is responsible for testing the relevant portions of the MACSIS application for their section. This testing usually involves parallel runs of production data for one week.

There were no program enhancements made to MACSIS in calendar year 2004.

Program Modifications

If a program modification is required, the Program Modification Log (BUG Log) is updated by Information Technology supervisors. This log is centrally maintained by ODMH/ODADAS to report and track the progress and status of all program modifications. The BUG log entry is sent to Perot and Ohio Project representatives by the supervisor who discovered the problem. Perot support personnel log and track the problem resolution internally.

Perot decides on the resolution strategy, assigns programmers and assigns the bug a tracking number. The tracking number is then communicated to MACSIS supervisors who update the BUG log.

Once the modification is completed, Perot sends the program fix to ODMH/ODADAS for testing and implementation.

Testing of program modifications is the responsibility of the Information Technology supervisor who requested the change. Testing, performed in a separate test environment limited to appropriate personnel within the Information Services section, often involves a rerun of the identical data processed when the problem was discovered. Testing plans and documentation are maintained by the claims, member, and finance sections for all program changes.

Once the program changes are tested and verified, notification is presented at the weekly MOM meetings. The MIS Information Technology supervisor moves all changes from the test environment to production.

Access to Diamond 725 production source and object libraries is restricted to authorized personnel. To help accomplish this, a restricted account is required to transfer test programs into the live environment.

All large enhancements and modifications are received from Perot in the form of a new release. Perot sends installation instructions and release notes to ODMH/ODADAS prior to each new release to ensure the upgrade is placed into production correctly.

Once testing of the program modifications has been successfully completed by ODMH/ODADAS and the fix is put into production, the Information Technology supervisor will move the BUG to the closed tab of the Program Modification Log to indicate that testing was successful and the issue has been resolved.

POP meeting minutes and technical notes are available on the Internet to the board and county users to notify them of any minor changes to the MACSIS system. Open and closed issues logs are also maintained on the Web for statewide issues reported to the Behavioral Health Operations Committee.

Training for major changes is available to the county board users on an as-needed basis or at user meetings. MACSIS management provides training to users when major changes are made to the MACSIS application or when MACSIS support desk calls indicate a lack of understanding of some aspect of the system.

An extensive amount of documentation including electronic format requirements, system guidelines, presentations, and reports, is available on the Web.

In CY 2004, ODMH initiated the Web Revision and Design Project (WRAD) to remove pre-HIPAA references and to ensure the documentation was current. The project resulted in updates to the majority of MACSIS-related documents available on the Web. Both major MACSIS user guides (Board

Member and Claims Operations Manuals) were updated extensively. Three formal e-alerts, called "HIPAA Alerts", were issued in 2004, primarily focusing on the closure of the MACSIS pre-HIPAA production environment.

IT Security

User access to the MACSIS application is authorized by appropriate personnel. For users to obtain access to the MACSIS application, a MACSIS Account Request form is signed by the user and approved by his or her supervisor. The form is forwarded to the MACSIS Technical Team where it is processed and maintained. The form specifies which application level of group access and capabilities should be granted to the user.

Confidentiality of data requirements have been appropriately considered by MACSIS management, documented, and distributed to users for their sign-off.

UNIX-level access is appropriately restricted, and authorized by appropriate personnel. UNIX access granted, approved, and documented is processed and maintained by OIT.

A reconciliation of users' access privileges is conducted annually by the Office of Information Systems (OIS) to confirm all user access to MACSIS programs and data is appropriate to their assigned job duties. Each year, OIS distributes a list of all users and their access privileges to the respective county boards to validate their need for this access.

Although the county boards are requested to notify the state when an employee is terminated, the boards often do not send notification. No formal termination procedures are in place for ODMH. A new "Guideline Pertaining to MACSIS" was drafted during CY 2004 and formally approved for adoption in CY 2005 to outline the state and board's communication responsibilities regarding MACSIS system access. ODADAS has formal termination procedures in place that include removing all UNIX and MACSIS access.

Security violation reports are captured and e-mailed to Customer Services for daily online review. Violation report documentation is maintained for approximately two quarters. All multiple failed logon attempts are reported and reviewed for further investigation. In addition, detection control alarms are enabled through UNIX to monitor security violations and will automatically e-mail the SDD Operating Systems Services & Support (OS3) group and ODMH MIS Information Technology when the failed logon threshold is exceeded.

All ODMH PCs are equipped with anti-virus software that is scheduled for weekly automatic updates. Incoming e-mail are also scanned.

ODMH and ODADAS have established policies and procedures to define guidelines for Internet, e-mail, and general online computer use. These policies include personal computer usage, World Wide Web activities, e-mail usage, and password/user id requirements. HIPAA security-related policies were developed, approved by the deputy director, and placed into effect in July 2003. Policies are available to MACSIS personnel through the ODMH intranet.

The ODMH Password and User ID Policy was created to comply with OIT statewide policy and HIPAA privacy regulations. The policy applies to all computer and communication systems owned or operated by ODMH and operating subsidiaries.

ODMH's Password and User id Policy includes the following guidelines for password administration:

- Contain at least one alphabetic and one non-alphabetic character.
- Be a minimum of six characters in length.
- Be changed every 90 days for critical systems and 30 days for any accounts with system administration privileges.
- Be prohibited from reusing a password for at least one calendar year.
- Be locked after three unsuccessful attempts to enter a password.
- Be tested at least once per calendar year based on a risk assessment.

UNIX passwords comply with the OIT's Systems Services Guide policy, with the exception of requiring a non-alphabetic character, password re-use, and failed login attempt thresholds.

A UNIX server is used by MACSIS to extract the latest Medicaid eligibility information from ODJFS and update the Diamond software. For a user to logon to the server, a unique user id and password are required. Community and ODADAS users can use telnet software, which requires a unique user id and password, to remotely login to this UNIX server. System password controls have been established for the UNIX system on the production servers that processes the MACSIS programs and data. The following describe the system parameters defined for those servers:

- All system passwords must be a minimum number of characters with proper password syntax, changed according to a pre-defined password lifetime, and unique for a minimum number of password changes.
- User accounts are locked after a pre-defined threshold of failed logon attempts.
- Inactive accounts are automatically disabled.

Notifications of excessive logon attempts are e-mailed to ODHM for review.

Once logged into the UNIX server, all users may access the main menu of the Diamond 725 application by entering a unique user id and password. From the Diamond 725 main menu, users may login, logout, or change their password. All Diamond 725 passwords must be changed after a pre-defined password lifetime. Users are logged off inactive terminals after a pre-defined period.

MACSIS application programs and data reside on seven different UNIX servers. These servers house the development, testing, and production environments for the MACSIS application. Diamond 725 provides application-level security that can restrict the users at the transaction level.

Access to Diamond system administrator privileges is restricted to authorized IT personnel. System administrators have the ability to change, add, or delete all data within the application. The Diamond superuser passwords are changed after a pre-defined password lifetime.

To authenticate to the SDD network via the Internet, a user can enter a SecureID code and a personal identification number (PIN). The SecureID code is generated by a SecureID card authorized to and carried by the user. A unique SecureID code is generated by a computer chip inside the card every 60 seconds. To initiate the login process, the user must enter the SecureID code displayed on the card along with a unique PIN. A SecureID code is known by only selected authorized users. All remaining authorized users are granted access by defining their ohio.gov-provided static IP address to the firewall software. Once the user is authenticated, they are granted restricted access based on the access rules that apply to their UNIX user ids. Also upon authentication, the system ensures an encrypted path between the remote device (SecureID card) and SDD to prevent the information from being read and interpreted during transmission.

UNIX superuser accounts are limited to authorized personnel to ensure that access to sensitive system software and utilities is appropriately restricted and monitored. Superusers perform various root-level functions related to the system manager, postmaster, webmaster, user help, network manager, or database administrator duties. All failed connection attempts are reviewed and investigated for inappropriate use of the superuser account. The OS3 group also maintains an encrypted system security password file. In the UNIX operating system, the system password file, where the user passwords are stored, is automatically encrypted, along with related password commands. The file is readable only by authorized personnel.

Application Level Access Controls

Diamond application passwords do not adhere to any of the standards established in the Password and User id Policy. All users must have a UNIX logon to access Diamond, which is the only application available to users on the server. A failure at the UNIX level would prohibit access to Diamond. Password parameters have been hard coded into the Diamond 725 system. Diamond only requires a minimum password length greater than one byte (character) and users are exited out of Diamond after three unsuccessful logon attempts; however, their account is not locked and does not have to be reset by an administrator.

Network Firewalls and Physical Security

Three of the MACSIS servers, functioning as the test, web service, and HIPAA production environment, are located at the State Office Tower (SOT). The remaining four servers, functioning as development, data warehouse, and other production environments are located at the State of Ohio Computer Center (SOCC).

Access to the production servers on the network is protected from unauthorized outside exposure by filtering routers and firewalls that are maintained on the Service Delivery Division (SDD) network.

Controls related to physical security, to the filtering routers and firewalls, and to the environment of the computer rooms, are performed by personnel of the SOT and SOCC, and are not the responsibility of ODMH or ODADAS management.

IT Operations

MACSIS batch processes are documented, scheduled, and maintained on an ongoing basis. Each morning, a file is sent from the Ohio Department of Job and Family Services (ODJFS) with the latest Medicaid eligibility information. The MACSIS servers and data files are updated through a nightly batch process. The batch jobs are manually initiated and logged by the operations staff. The log records batch processes that must be run at specific times (e.g. daily, weekly, monthly, yearly). The log documents the files created, the frequency of files created, date and times for each job started and stopped, and a record count of records processed on each job. The log is maintained in Operations for a month and then sent to the Patient Billing and Reimbursement section and retained for approximately two years.

The IBM system software upgrades and releases are selected based on user need and performance of the upgrade. All new upgrades to system software are tested by the vendor prior to release. The prior release is kept for approximately three to six months and can be restored easily if an upgrade causes a problem. Installation procedures and a check list are available to control the system upgrade process.

IBM Tivoli Storage Manager, TSM, is used to automatically schedule and maintain backup and recovery. Incremental data file backups are

performed automatically on a nightly basis on all seven test and production servers. Incremental backup cartridges are stored in a robotic tape silo. TSM is configured to help ensure that any file or all files can be restored to any date/time within 30 days. Users can request tests be performed on their specific backup files.

TSM maintains each data file in storage for 30 days if the storage file has been updated. If the data file in storage does not have an update within 30 days, TSM will store the file indefinitely until an update is received. If a storage file is deleted from production, TSM will maintain the file for 120 days. A log of the TSM incremental backups is created with each run and retained for a period of seven days. Determination of successful backup is the responsibility of MACSIS management.

Off-site incremental system backups are performed automatically on a daily basis and maintained at the opposite server location. Each day, a job is run through TSM at both the SOT and the SOCC. The job copies the incremental daily backup storage data files of the SOT servers to the TSM at the SOCC. The job also copies the daily backup storage data files of the SOCC servers to the TSM at the SOT. The receiving TSMs will then copy the dual copy of the storage files to cartridges in their respective robotic tape libraries for off-site storage (i.e. the SOT tape library cartridges contain backup files for SOCC servers, and the SOCC tape library cartridges contain backup files for the SOT servers).

APPLICATION CONTROLS

Multi-Agency Community Services Information Systems (MACSIS)

Background

MACSIS is designed as a central benefits administration system and is accessed by community boards and board consortiums across the state. The MACSIS system replaced the summary level reporting systems, Mental Health Information System (MHIS), Alcohol and Drug Client Data System (ADCDS), and the Community Medicaid billing systems.

Community boards have access to the system through a state telecommunication network to the software, which provides for eligibility checking, enrollment, service assessment, billing, and outcome monitoring functions. The system is HIPAA-compliant and designed to meet ODJFS and federal reporting requirements.

Overview

MACSIS is an information system that allows ODMH, ODADAS, and their local boards to manage, measure, and monitor the service utilization of Medicaid, state, and local public funds.

MACSIS consists of the following five components:

1. The pre-processor programs, Overnight First Pass, Diamond Data Services (DDS) and BeMIS that perform the claims EDI process, electronic transfer of claims data, the validation of claims submitted, a file management process, the translation of claim data into MACSIS-readable format, and the forwarding of claims EDI for processing to Diamond 725.
2. The Diamond 725 system that includes membership management, provider contract management, claims adjudication processing, accounts payable, remittance advice, and interface to board financial and/or county treasurer systems.
3. The Medicaid eligibility system that updates the Diamond system daily to manage Medicaid and non-Medicaid plan assignments and eligibility periods.
4. The Medicaid reimbursement process that extracts the Medicaid billable services from Diamond 725, translates them into Medicaid billing format for both ODMH and ODADAS, and processes claims through ODJFS. It also posts remittance advice data back into the Diamond 725 system and reimburses boards for Federal Funding Participation (FFP) services they have purchased.
5. The board financial systems that extract accounts payable data from Diamond 725 to board financial systems and forwards it to the county treasurer.

Claim Submission Process

The submission process refers to the flow of claims data submitted by agencies and hospitals through the MACSIS system for purposes of adjudication at the board or state level.

This process involves many steps and levels of eligibility verification and claims adjudication, including the following:

1. Verification of Client Eligibility

This step involves the agency or hospital's verification of client eligibility to receive services and must be completed prior to the submission of a claim. Community boards are responsible for administering the process by which clients are enrolled on MACSIS and for instructing agencies and hospitals on how to verify eligibility. MACSIS receives automatic nightly updates of eligibility information from ODJFS's eligibility system (MMIS).

2. Electronic Transmission of Claims

This step involves the process of an agency or hospital submitting claims electronically to their designated board for forwarding to MACSIS. Agencies or hospitals can submit this information via a board-supported system, third party billing service, or interface from their own billing system. The claims submitted include services for both community Medicaid and non-Medicaid (i.e. other publicly-funded) programs.

3. Board-Level Claim Adjudication and Remittance

Each board transfers incoming agency/hospital claim files to MACSIS, which is used to adjudicate claims for payment according to the contracts and agreements the boards have established with their agencies or hospitals. In some instances, payment for services rendered is pre-distributed by the boards and, in other cases; payment is made upon receipt of the claim as pre-defined by the board and agency/hospital contract or agreement. In all cases, a remittance report generated by the board accompanies payment. With MACSIS, boards are required to remit 100% of the contracted payment for community Medicaid services to the agency prior to the receipt of the Federal Financial Participation (FFP) reimbursement from ODJFS.

4. ODMH/ODADAS Claim Adjudication

For community Medicaid services only, ODMH and ODADAS forward the MACSIS claim information to ODJFS in the required format for adjudication and determination of the FFP reimbursement.

5. ODJFS Claim Adjudication and Remittance

For community Medicaid services only, ODJFS adjudicates the claims for the determination of eligibility and the calculation of the FFP reimbursement. ODJFS performs the appropriate transfer of funds to reimburse ODMH/ODADAS for the previously distributed portion of the claim payment. ODMH and ODADAS provide the boards with the related remittance information.

Input, Processing, and Output Controls

County boards are responsible for contracting with providers who have Medicaid contracts, and for deciding upon fees for service (purchase of service and grant based funding), case rates, and capitation agreements. When a provider determines that payment for behavioral health services on behalf of a new client will be funded in part or in whole by a board, the client is enrolled in the MACSIS system. Each board establishes a single point of enrollment for new clients, which will collect the information necessary to enroll the client. All clients who are served with public funds (federal, state, or local levy) must be enrolled in MACSIS.

Upon enrollment, clients will be assigned a Unique Client Identifier (UCI) which must be used when submitting claims. These client identifiers are sequentially assigned and unique per individual throughout the state. This number will remain the same for the client even if subsequent services are provided by another board, and will be used to link the client to their current Medicaid Recipient Number if one exists. A generic "pseudo" UCI number will be assigned for purposes of billing non-client specific services when appropriate.

Boards enroll contracted providers in MACSIS, which automatically assigns provider IDs. Providers can be a person, place, or organizational group. Each provider site with different rates will have a universal provider Id (UPI). A valid UPI must be submitted on each claim prior to processing.

Professional behavioral health service claims must be submitted electronically to the boards in a HIPAA-compliant format, as currently required under HIPAA. Inpatient facility psych claims are not currently being submitted or processed through the MACSIS system. Although a handful of boards manually enter claims into MACSIS to reimburse providers for inpatient stays, the majority of boards pay for private inpatient psych care outside of MACSIS.

Providers are required to roll up claims for each date of service for a client by procedure code and modifier before submission to help reduce the instances of possible duplicates.

Claims undergo various levels of edit checks before file conversion by Overnight First Pass processing and adjudication by Diamond 725.

Providers must submit all electronic claim files to the boards. Boards are required to:

- Log files received with the number of claims and total billed dollars.
- Ensure the file name is compliant with naming standards.
- Open the file to ensure the file is not corrupted.

Claims must be submitted for a contracted service by a certified provider. All claims must contain a valid modifier and diagnosis code when submitted by the provider for payment.

Each submitter (board) has a designated directory where all files for that board are stored. On a daily basis, boards can forward files to this input directory in suspense, while waiting for the Overnight processing.

Prior to MACSIS adjudication, the state's Overnight First Pass process performs multiple checks to ensure the integrity of the claims, in addition to ensuring they are compliant with the 837P National Standards format. Non-compliant claims are rejected. Duplicate checking is performed within Diamond and boards are no longer required to pre-check incoming claims. Overnight First Pass will then run programs against files in the input directory and move them to the correct location for adjudication.

Modifiers are used to qualify how services are provided. They are used by MACSIS to determine what is billable to Medicaid. MACSIS will determine if a client is Medicaid eligible but a modifier will determine if Medicaid covers the service.

It is the board's responsibility to transfer electronic claim files from the providers to MACSIS. The board must also ensure that claims are processed and adjudicated in a timely manner and that payment and supporting remittance advice information is sent back to the provider. Response to inquiries about eligibility or claim status and payment are made by the board. The board must establish and manage claims adjudication policies for non-Medicaid services under the board's jurisdiction. They also ensure that the system setup complies with these policies and coordinate provider number assignment and entering of contract rates and information for non-Medicaid services in MACSIS. MACSIS will determine the correct contracted rate and information for each claim based on the UPI, procedure codes, and pricing schedule.

On a weekly basis, the claim files held prior to processing are converted to a format required for Diamond 725 processing. If the converted file cannot be processed, it is moved to the reject directory for investigation and resolution.

If the program is successful in converting the files into a readable format, a MACSIS utility program will place the files into a directory, ready for processing by the Diamond claims EDI process. Throughout this process, the files remain associated with the submitter and are processed separately.

All valid records are deposited by Overnight First Pass into a directory on the Diamond system for each submitter. The submitter process is run for each Board on a pre-defined schedule. MACSIS production control runs the claims EDI process for each board. Edits exist within Diamond 725 to help ensure that authorized transactions are accurately recorded. Claims EDI produces a series of reports in edit mode that can be reviewed by each board. The boards authorize the posting of the Claims EDI process.

Edit checks are performed by Diamond 725 during claims EDI processing to help identify and deny duplicate claims. Any claim with the same procedure code and modifier combination will be denied. Additionally, benefit rules are in place that limit and deny partial hospitalization services when the daily eligibility limits for adults and children are reached.

MACSIS will accurately process claim information based on pre-authorized input criteria. The provider must initiate the accurate enrollment of the client on the MACSIS system prior to submission of claims for services rendered. It is also the provider's responsibility to ensure the accurate and timely submission or re-submission of claims for services rendered and to comply with the submission requirements.

The Medicaid eligible claims from Diamond are put into the Medicaid billing format and sent to ODJFS for processing. A separate provider number is used to distinguish between ODMH and ODADAS in the MACSIS system. All other processing is identical to the Medicaid Billing process.

Medicaid adjudicates the claims and reports the disposition of the claims back to MACSIS. Most are either paid or rejected and some are held. The ARA - Medicaid Remittance Advices are then returned to ODMH/ODADAS by ODJFS for MACSIS to reconcile all rejected Medicaid claims against the submitter's account.

A pay tape containing the prior week's ARA Medicaid Remittance Advices is posted weekly back into the Diamond System. The ARA File is linked back to the original claim line in Diamond. A reversal for all rejected claims is completed. ARA reports for each board report how each claim line was adjudicated by MACSIS/ODJFS.

All reports (for Medicaid and non-Medicaid) are placed in a report directory that is assigned to each submitter. These reports indicate critical errors,

warnings, rejections, and other problems that occurred during the claims EDI process. The board is responsible for reviewing and working these reports. In most cases, the board prints the reports locally and distributes them to their claims group for resolution.

Pricing schedules are used by MACSIS to determine the correct amount for Medicaid and non-Medicaid services based on UPIs. Non-Medicaid contract rates and information are entered by each board and should be reflective of the original contracts with each provider.

Medicaid rates and information are maintained at the state level and are entered by authorized personnel. Rate sheets are submitted by the providers to the boards, who then forward the sheets to the state. The state manually keys all information directly into the Diamond 725 pricing schedules. Any time that adjustments to Medicaid pricing schedules must be made, a new rate sheet is submitted by the provider to the board.

Procedure codes used to identify Medicaid billable services are updated by authorized personnel. These codes allow MACSIS to identify all Medicaid claims during the EDI process for submission to ODJFS. If a new procedure code is submitted on a rate sheet, MACSIS personnel will contact the Certification Office for verification and approval of the new procedure code.

Changes to client Medicaid eligibility are verified for completeness and accuracy. MACSIS maintains a DB2 file, MEDELIG, that contains Medicaid eligibility information for all clients. ODJFS maintains Medicaid eligibility data in the Recipient Master File (RMF). Each morning, ODJFS allows MACSIS to access the RMF file and import any changes that were made to existing recipients within the last 24 hours, into the DB2 eligibility file. DB2 also receives information from the Diamond 725 application to update the databases with current information from Diamond 725.

Each night, a file is created in DB2 containing updated recipient and Medicaid information and is imported into Diamond 725 as an FTP file. An Update Run Daily log is manually completed each morning to confirm that the RMF file was successfully read into DB2. A Summary Control Report is created to verify that the total number of records updated from the DB2 MEDELIG file is reconciled to the total records written to Diamond 725.

Weekly procedures exist to detect and resolve discrepancies in Medicaid eligibility information from the MACSIS MEDELIG file and the ODJFS RMF file. Exception reports are produced to notify the Membership Maintenance Group of discrepancies between the MEDELIG and RMF files. The Maintenance Group then researches and resolves the exception report items.

If the board or provider needs to resubmit a claim due to errors in the original submission, the original claim specifications apply. An additional re-submission claim number or transaction control number is not required. MACSIS will identify the resubmitted claim by matching several key data elements on the claim to existing claims. For resubmitted claims, units of service and dollar amounts cannot be adjusted and auto adjudicated in MACSIS but must be manually adjudicated by the board.

Each board is responsible for adjusting the original claim and adjudicating the resubmitted claim in MACSIS via a manual process.

Once claims are submitted for processing in MACSIS, access to accumulated data is restricted to authorized personnel. All other board or state administration users are restricted from viewing claims before the claims have been adjudicated.

After the claims have been adjudicated, all users are restricted to only view history screens that will display the status of the claim. No modifications to historical claims are permitted after the claims have been finalized by Diamond.

USER CONTROL CONSIDERATIONS

The ODMH and ODADAS's MACSIS application was designed with the assumption that certain controls would be implemented by user agencies. This section describes additional controls that should be in operation at the user agencies to complement the controls at the ODMH and ODADAS. User auditors should consider whether the following controls have been placed in operation at user organizations:

Related to General Controls

- User boards should be aware of the confidential nature of system and network passwords and should take precautions to ensure passwords are not compromised.
- When user board personnel leave or are otherwise terminated, all access capabilities for that user should be immediately removed or modified. A message should immediately be sent to the MACSIS personnel notifying them of the vacancy and that any direct or remote access to the system should be revoked.
- User boards should have a documented acceptable computer use policy to define what activities are deemed appropriate for their users of the Internet. Internet users should be required to acknowledge and accept the terms of the policy before access is provided.
- User boards should ensure all network user ids are individually assigned to each system user to improve individual accountability to user activity.
- User boards should ensure system and network level user ids and associated privileges and attributes are issued only to authorized users who need access to computer resources in order to perform their job functions.
- User boards should be aware of the confidential nature of MACSIS passwords and should take precautions to ensure passwords are not compromised.
- User boards should ensure that MACSIS user ids, passwords, and associated privileges for their board personnel are issued only to authorized users who need access to computer resources in order to perform their job function.
- User boards should ensure all user ids at the application level for their personnel are individually assigned to each system user to improve individual accountability of user activity.
- Network and communication lines, junctions, and key hardware components should be secured in an area that restricts access to only authorized IT individuals.
- User boards should retain source documents for an adequate period to ensure data can be re-entered in the event that data files are destroyed prior to being backed-up and rotated off-site.
- User boards should ensure that backup and off-site rotation procedures for application programs and data are adequate for their objectives and compliance with established data retention schedules.

Related to Application Controls

- Access to perform MACSIS transactions should be restricted to only those individuals whose job responsibilities require it.
- Transactions should require supporting documentation with proper approval.
- All user boards should follow established guidelines for performing duplicate claim checking.
- After posting claims, user boards should review the Process EDI (PREDI) post report and resolve the error messages.
- User boards should review input subdirectories (key control totals within input files, production files, NSF and ANSI rejected files, reports, and archive files) to determine that submitted claims were processed completely by the Overnight program and forwarded to the MACSIS system for adjudication.
- User boards should review all remittance advice reports (for Medicaid [ARA] and Non-Medicaid [ERA]) placed in the report directory by MACSIS to ensure critical errors, warnings, rejections, and other problems that occurred during the Claims EDI process are resolved.
- User boards should ensure that claims are processed and adjudicated in a timely manner.
- User boards should confirm that claims submitted for processing reflect provider contracted rates and information in MACSIS.
- Access to perform non-Medicaid contract rates maintenance activity should be restricted to only those individuals whose job responsibilities require it.
- Periodic reviews of the non-Medicaid and Medicaid contract rate data should be performed at each board to verify that contract activity is authorized and valid.
- User boards should follow guidelines established for adjusting the original claim and adjudicating the resubmitted claim via a manual process.
- Access to the claim history file should be restricted to “view” to only those individuals whose job responsibilities require it.
- Computer users should be aware of the confidential nature of passwords and should take precautions to ensure passwords are not compromised.
- For all payable claims, board staff should reconcile the number of claim lines/dollar amount submitted against what was received, accepted, rejected, etc.

The user control considerations presented above do not represent a comprehensive set of all the controls that should be employed by user agencies. Other controls may be required at user agencies.

SECTION III - INFORMATION PROVIDED BY THE SERVICE AUDITOR

This section is intended to provide interested parties with information sufficient to obtain an understanding of those aspects of the ODMH's and ODADAS' internal control that may be relevant to member community's internal control, and reduce the assessed level of control risk below the maximum for certain financial statement assertions.

The broad objectives of data processing controls should be achieved by a combination of the procedures that are employed in various segments of the transaction processing system for example procedures performed at the ODMH and ODADAS and procedures performed at user boards which utilize the ODMH and ODADAS.

For each of the control objectives listed below, only those controls which contribute to the attainment of the related control objective are described and were tested.

GENERAL EDP CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS

Overall Operation of the IT Function

<p>Overall Operation of the IT Function - Control Objective: IT Personnel - IT personnel should have the appropriate knowledge and experience for the complexity of the IT environment.</p>		<p>Control Objective Has Been Met</p>
<p>Control Procedures:</p>	<p>Test Descriptions:</p>	<p>Test Results:</p>
<p>ODMH and ODADAS use job descriptions and organizational charts to define the various IT roles and responsibilities.</p>	<p>Inspected the ODMH and ODADAS organizational charts and job descriptions.</p>	<p>The ODMH organizational chart segregated various IT positions that reported to two data systems assistant administrators.</p> <p>The ODADAS organizational chart reflected the mainframe programming, PC, network, and the data production units.</p> <p>ODMH and ODADAS developed job descriptions that included an overview of the duties an employee in each position was expected to perform. The job descriptions listed the minimum acceptable characteristics expected for an employee to be able to adequately perform the job.</p>

Overall Operation of the IT Function - Control Objective: IT Personnel - IT personnel should have the appropriate knowledge and experience for the complexity of the IT environment.		Control Objective Has Been Met
Control Procedures:	Test Descriptions:	Test Results:
ODMH and ODADAS provide training to the IT staff to help ensure they have the skills necessary for the complexity of the IT environment.	Inspected documentation of the training courses attended by various IT staff.	The ODMH and ODADAS training documentation listed training provided to the IT staff throughout the audit period.
IT management meets periodically to discuss and oversee the IT function and its related activities.	Inspected the Project and Operations Planning (POP) meeting minutes.	The POP meeting minutes outlined the following: <ul style="list-style-type: none"> ▪ The date of the meeting. ▪ A list of individuals who attended the meeting. ▪ A list of topics discussed. ▪ The date, time, and place of the next POP meeting.

Overall Operation of the IT Function - Control Objective: IT Planning - IT strategy should be consistent with the overall strategy of the organization.		Control Objective Has Been Met
Control Procedures:	Test Descriptions:	Test Results:
ODMH and ODADAS developed a long-range information technology plan to help ensure future IT personnel, hardware, and software issues are addressed.	Inspected the ODADAS and ODMH FY 04-05 long-range information technology plans to determine whether they contained the following: <ul style="list-style-type: none"> ▪ Ties to forecasted growth objectives. ▪ Projected needs for personnel, hardware, and software. ▪ Periodic updates to address the progress obtained with the various objectives. 	ODADAS and ODMH information technology plans for FY04-05 contained the agencies' goals. The strategic plans included mission and vision statements, business program areas, business drivers, agency business goals and business objectives, and an organizational assessment. The tactical plan included application maintenance activities, infrastructure maintenance activities and IT projects.

Changes to Existing Applications or Hardware Systems

<p>Changes to Existing Applications or Hardware Systems - Control Objective: Change Requests - Requests for application program changes or system upgrades should be appropriately considered and processed.</p>		<p>Control Objective Has Been Met</p>
<p><i>Control Procedures:</i></p>	<p><i>Test Descriptions:</i></p>	<p><i>Test Results:</i></p>
<p>ODMH/ODADAS maintains a software maintenance agreement with Perot for the MACSIS application residing on the UNIX servers.</p>	<p>Inspected the software support agreement for the MACSIS application as well as proof of contract payment.</p>	<p>An invoice was sent and paid to the vendor in October 2003 for support services for the period of July 1, 2003 through June 30, 2004.</p> <p>Because new contract terms between the client and the state of Ohio were not agreeable, a new contract was not signed by the vendor. As of March 2005, ODMH and ODADAS were working to bring the terms in front of the Controlling Board for consideration and negotiation.</p>
<p>Perot provides release notes to ODMH/ODADAS with each MACSIS upgrade to give management a description of the changes and to assist them in making informed decisions regarding implementing the upgrades.</p>	<p>Inspected the release notes for version 8.3.1 F to help ensure a description of the changes contained within the new release was provided.</p>	<p>The release notes for version 8.3.1F included installation instructions, and other related documentation. The installation instructions walked through the installation process and post-installation procedures.</p>
<p>A Program Modification Log is centrally maintained by ODMH/ODADAS to report and track the progress and status of all program modifications.</p>	<p>Inspected the Program Modification Log of all BUGs reported in calendar year 2004 to determine that each change was evaluated, prioritized, and monitored.</p>	<p>The Program Modification Log was located on an ODMH/ODADAS network drive and was accessible to all network users.</p> <p>The Program Modification Log listed the date the issues were reported, as well as key progress and status information for the changes tracked.</p>

Changes to Existing Applications or Hardware Systems - Control Objective: Testing of Program Changes or Hardware System Upgrades – Program changes and hardware system upgrades should be tested to ensure that they achieve the business’ requirements and do not negatively impact existing processing.		Control Objective Has Been Met
Control Procedures:	Test Descriptions:	Test Results:
Test plans are developed and documentation is maintained for all program changes.	Inspected the claims, member, and accounts payable sections’ test plans and documentation for the upgrade from version 8.3.1 d to version 8.3.1 f (the only change made to production during the audit period).	Test plans and documentation relating to the upgrade from version 8.3.1 d to version 8.3.1 f of the MACSIS Diamond 725 software were maintained by the three users groups involved with the processing of MACSIS.
Access to Diamond 725 test source and object libraries is restricted to authorized personnel within the information services section.	Inspected the UNIX user ID listing of individuals with access to the test environment.	All user IDs with access to the test server were required and appropriately restricted.

Changes to Existing Applications or Hardware Systems - Control Objective: Transfer into the Live Environment - The transfer of programs or system upgrades into the live environment should be appropriately controlled.		Control Objective Has Been Met
Control Procedures:	Test Descriptions:	Test Results:
Perot sends installation instructions and release notes to ODMH/ODADAS prior to each new release to ensure the upgrade is placed into production correctly.	From the list of all releases and patches that were put into production during calendar year 2004, chose the only change to production during the audit period and inspected the installation instructions and release notes.	Perot sent several documents for the upgrade to version 8.3.1 f. Among the documents were installation instructions and a list of fixes included in the new upgrade.
Access to Diamond 725 production source and object libraries is restricted to authorized personnel.	Inspected the Diamond UNIX account values to determine if the Diamond user account restricted all direct and remote logins, and that the switch user (su) command was the only way to access this account. In addition, reviewed a list of the groups and users within those groups with access to su to the Diamond account.	Diamond account parameters did not allow a user login or login remotely (rsh, telnet or rlogin). However, su from another user account was permitted. Only one group ID was permitted to su to the Diamond account. All group members were authorized and required access to perform this function. FTP was also allowed, however can only be used for file transfers and still required the user ID and password.

<p>Changes to Existing Applications or Hardware Systems - Control Objective: Documentation and Training - Technical documentation should be updated to reflect program changes and system upgrades. When changes to applications and system upgrades affect user procedures, documentation should be updated accordingly. Likewise, users and IT staff should receive appropriate training when their responsibilities are impacted by application changes or system upgrades.</p>		<p>Control Objective Has Been Met</p>
<p>Control Procedures:</p>	<p>Test Descriptions:</p>	<p>Test Results:</p>
<p>POP meeting minutes and technical notes are available to the board and county users to notify them of any minor changes to the MACSIS system.</p>	<p>Inspected the POP meeting minutes and the technical notes via the ODMH web site.</p>	<p>POP meeting minutes and technical notes were maintained on the Internet for CY 2004. POP meetings were held monthly with the exception of June, August and October. Each month's minutes were recorded and included such items as topics discussed, special project updates, user group updates, board global issues, and plans for the next meeting.</p> <p>There were 14 technical notes/documents maintained and available in CY 2004. The documentation included access request forms and statuses, confidentiality forms, a listing of FTP accounts and directories, a link to a website that determines your IP and trace-route path, updates on the HIPAA notify program, the layout of the claims post report, and information from the extract of claims from the HIPAA environment from the affiliation file, claims, member, and new and old claims and member layouts.</p>
<p>MACSIS management provides training to users when major changes are made to the MACSIS application.</p>	<p>Inspected the documentation of the claims, member, and MIS user group trainings as well as the contacts, pricing and adjudication training for calendar year 2004.</p>	<p>The claims user group training was held in April 2004. The member user group training was held in May 2004. The MIS user group trainings were held in August 2004. The contracts, pricing and adjudication training was held in July 2004.</p>

IT Security

IT Security - Control Objective: Security Management – Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data		Control Objective Has Been Met
Control Procedures:	Test Descriptions:	Test Results:
User access to the MACSIS application is appropriately restricted and authorized.	From a list of all UNIX users added during CY2004, selected 10 new users and inspected their corresponding MACSIS access request forms for staff signature, supervisor signature, and MIS personnel signature.	No relevant exceptions noted.
Confidentiality of data requirements have been appropriately considered by MACSIS management, documented, and distributed to users.	From a list of all UNIX users added during CY 2004, selected 10 new users. Inspected the disclosure of information forms for a user signature.	No relevant exceptions noted
UNIX-level access is appropriately restricted, and authorized.	From a list of all UNIX users added during CY 2004, selected 10 new users, and inspected their TCP/IP access request forms for access rights and supervisory approval.	No relevant exceptions noted.

IT Security - Control Objective: Security Management – Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data		Control Objective Has Been Met
Control Procedures:	Test Descriptions:	Test Results:
A reconciliation of users' access privileges is conducted by the Office of Information Systems (OIS) on an annual basis to confirm that all user access to MACSIS programs and data is appropriate to their assigned job duties.	Obtained the Office of Information Services' (OIS) list of counties/boards that had user accounts e-mailed to them for verification of access to MACSIS. Selected 8 counties/boards and reviewed any changes on the requests to help ensure that changes in access were updated accordingly on the UNIX file and the MACSIS system administrator access grouping.	All access request responses were acknowledged and completed. All of the accounts that were requested to be deleted had been removed from the UNIX server user file.

IT Security - Control Objective: Security Management – Management should ensure the implementation of access control policies, which are based on the level of risk arising from access to programs and data		<i>Control Objective Has Been Met</i>
<p>Detection control alarms are enabled through UNIX to monitor security violations and will automatically e-mail the SDD OSSS Group and the ODMH MIS Information Technology Supervisor when the failed logon threshold is exceeded.</p>	<p>With the assistance of ODMH MIS, entered four failed logon attempts and inspected the corresponding e-mail notification and follow-up of the security violations.</p> <p>Note: During CY 2004, the failed logon threshold was set to 13 and was not updated to 4 attempts until March 2005.</p> <p>An additional e-mail notification from CY04 was obtained and inspected to help ensure that prior to the update, e-mail notifications were sent.</p>	<p>An e-mail notification was received noting the four failed logon attempts and related information.</p> <p>The e-mail notification that was sent prior to the update of the logon threshold contained the same information as the e-mail mentioned above for failed logon attempts greater than 13.</p>
<p>ODMH/ODADAS established policies and procedures to define guidelines for Internet, e-mail, and general online computer use.</p>	<p>Inspected the ODMH policies on Internet, e-mail, web, and general online computer use.</p>	<p>The ODMH policies provided all ODMH offices and employees with guidelines regarding the appropriate use of Internet activities, the responsibility of agency management to manage Internet servers and electronic mail services, and the personal responsibility of state employees using the Internet, electronic mail services, and online services. The policies were available to all employees online at the MACSIS intra-web.</p>

IT Security - Control Objective: System Level Access Controls - Access to the computer system, programs, and data should be appropriately restricted.		Control Objective Has Been Met
Control Procedures:	Test Descriptions:	Test Results:
System password controls have been established for the UNIX system on the production servers that process the MACSIS programs and data.	Inspected the password parameters file of all users on the MACSIS production server using ACL audit software.	One system account (ldap) used by the SDD OSSS group did not have any password parameters defined because when software was installed, the account was created using the UNIX defaults.
System sign-on parameters have been established to prevent a high number of failed sign-on attempts.	Inspected the system sign-on parameters for all users on the MACSIS production server using ACL audit software.	One system account (ldap) used by the SDD OSSS group did not have any password parameters defined because when software was installed, the account was created using the UNIX defaults. One user account did not have the sign-on parameter defined; however, when the SDD OSSS group was made aware of the absence of the parameter for the user account, they immediately updated the account to limit the parameter to five.

<p>IT Security - Control Objective: System Software and Utilities Access Controls - Use of master passwords, powerful utilities, and system manager facilities, should be adequately controlled.</p>		<p>Control Objective Has Been Met</p>
<p>Control Procedures:</p>	<p>Test Descriptions:</p>	<p>Test Results:</p>
<p>UNIX super user capability is limited to authorized personnel to help ensure access to sensitive system software and utilities is appropriately restricted and monitored.</p> <p>An alert is sent to management when successful or failed attempts were made to switch user (su) or logon as root.</p>	<p>Inspected the Login/Logout Activity Log for December 2004 to confirm only authorized personnel logged into the system as root.</p> <p>In addition, observed an OS3 group member complete a successful and a failed attempt to su to root. After the attempts, inspected the e-mail notification of the successful and the failed connection attempts to switch user to root.</p>	<p>The Login/Logout Activity Log displayed successful attempts to logon as root during the time period. The addresses of the users attempting to login as root belonged to authorized members or workstations.</p> <p>The OS3 group member completed one successful and one failed attempt to su to root. Both attempts generated an e-mail notification to the OS3 group indicating the successful and failed attempts.</p>
<p>Access to the encrypted UNIX security password file is appropriately restricted to authorized personnel.</p>	<p>Inspected the access privileges to the encrypted UNIX password file.</p>	<p>The encrypted password file was owned by authorized IT personnel only. Root had READ and WRITE access only to the file. The file had no Group or World access.</p>
<p>Access to Diamond system administrator privileges is restricted to authorized IT personnel.</p>	<p>Inspected the Key Word Security Groups Listing and the System Administration Access Grouping.</p>	<p>All personnel were restricted to None or READ-only privileges for all system administrator functions. The only exception was an authorized administrative account with WRITE and DELETE access.</p>

IT Operations

IT Operations - Control Objective: System Administration and Maintenance - Appropriate procedures should be established to ensure that the system is properly maintained and monitored.		Control Objective Has Been Met
Control Procedures:	Test Descriptions:	Test Results:
MACSIS batch processes are documented, scheduled, and maintained on an ongoing basis.	Inspected 24 Daily Run Logs for evidence that batch jobs were documented, scheduled, and maintained on an ongoing basis. The Daily Run Logs selected were for the 7th and 13th day of each month.	All of the Daily Run Logs documented batch jobs that were run daily. Each log listed the date run, job number, start/end times, in/out record counts, and any error counts.
System availability/downtime for all MACSIS servers is monitored and maintained by Operating Systems Service and Support (OS3) management on an ongoing basis.	Inspected the system availability reports for October, November, and December 2004.	System availability reports were maintained by OS3 staff and were available for review by OS3 management and respective clients. The reports outlined the percentage of availability and downtime of the UNIX system services.
IT Operations - Control Objective: Backup - Up-to-date backups of programs and data should be available in emergencies.		Control Objective Has Been Met
Control Procedures:	Test Descriptions:	Test Results:
Nightly incremental backups on all MACSIS servers are performed automatically.	Inspected the nightly backup logs for the week of 2/22/05 through 2/28/05 and the week of 2/7/04 through 2/13/04 for evidence the incremental backups were performed nightly. Inspected the Query Filespace Command Output Report showing all the production backup files in the SOCC robotic tape library as of 2/28/05.	All logs contained successful completion statements for the nightly MACSIS backups. The Query Report displayed file information on the 31 backup files stored in the tape library. The query listed the node name, file space name, filespace ID, platform name, filespace type, and the size of the files.

IT Operations - Control Objective: Backup - Up-to-date backups of programs and data should be available in emergencies.		Control Objective Has Been Met
Control Procedures:	Test Descriptions:	Test Results:
<p>Off-site incremental system backups are performed automatically on a daily basis and maintained at the opposite server location.</p>	<p>Inspected the Tivoli Storage Manager (TSM) job schedule for the daily off-site dual server backups.</p> <p>Also, inspected the status of administrative backup tasks for the week of 2/22/05 through 2/28/05 for indication of successful completion.</p>	<p>A daily job was scheduled to run that produced a dual copy of the daily backup tapes. The off-site dual copy job was implemented in September 2002 and did not have an expiration date. The status of the off-site dual copy job was ACTIVE, indicating the job was set to run daily.</p> <p>For the week tested, the administrative task list contained the scheduled start date and time, the actual start date and time, the schedule name, and the status of the scheduled task. The dual backup copy had a "completed" status.</p>

APPLICATION CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS

Multi-Agency Community Services Information System (MACSIS), Diamond 725, Version 8.3.1F

<p>MACSIS - Control Objective: Authorization: Information entered into the entity's computer application represents valid data approved by the entity's management.</p>		<p>Control Objective Has Been Met</p>
<p>Control Procedures:</p>	<p>Test Descriptions:</p>	<p>Test Results:</p>
<p>Only authorized claim data is submitted for further processing.</p>	<p>Inspected the MACSIS Member Field Descriptions listing to verify a valid Unique Client Identifier (UCI) must be utilized when submitting a claim for payment or credit. Also inspected the PREDI error codes listing as well as a summary of critical errors to help verify edits were in place to require valid UCI's.</p> <p>Inspected the MACSIS 837 Professional Claim Informational Guide to help verify that a valid UPI must be submitted on each claim prior to processing. Also inspected the PREDI error codes listing to verify edits were in place to require valid UPI's</p> <p>Inspected the claims EDI file processing timeline for 837P in MHHIPPA for steps to validate authorized claims being submitted from boards.</p>	<p>The UCI or Subscriber ID was a sequential 12 character numeric field assigned by Diamond during enrollment (via EDI or manually). This field is required by both the system and the state.</p> <p>System documentation confirmed the use of edits to prevent unauthorized subscriber and provider identification numbers.</p> <p>The claims EDI file processing timeline for MACSIS claims contained various steps that validated the authorization of claims being submitted including the format, filenames, and claim type.</p>

MACSIS - Control Objective: Completeness of Input: All authorized transactions are input and accepted for processing by the application.		Control Objective Has Been Met
Control Procedures:	Test Descriptions:	Test Results:
Edit checks are performed by Diamond 725 during claims EDI processing that help identify and deny any duplicate claims.	<p>Entered a batch of claims into the ADTEST test region. Inspected a Diamond Claims EDI Detail Claims Report that detailed the claims entered. Also inspected the Post-EDI Transaction Set Job Log.</p> <p>The same claims (with the same patient number, billed amount, and service date already entered and processed by EDI in the first run) were re-entered into the test region. Inspected a second Diamond Claims EDI Detail Claims Report and Post EDI Transaction Set Job Log.</p>	<p>The Claims EDI Job Log of the first run of claims indicated that 'duplicate checking was turned on for this transaction. The detail claims report for this first run listed all claims entered. The Post EDI Transaction Set Job Log indicated all claims written to production in the first run were allowed.</p> <p>After the second pass through with the same claims, the claims EDI job log indicated 'duplicate checking was turned on for this transaction.' The Post EDI Transaction Set Job Log indicated all claims entered during the second run were denied because they were duplicates.</p>

MACSIS - Control Objective: Accuracy of Input: Authorized transactions are accurately recorded and in the proper period.		Control Objective Has Been Met
Control Procedures:	Test Descriptions:	Test Results:
Edits exist within Diamond 725 to help ensure authorized transactions are accurately recorded.	<p>Inspected the following reports from February 2004 for evidence of edits in place:</p> <ul style="list-style-type: none"> • PREDI Claims Batch Error Messages listing. • Diamond Claims EDI Critical Errors Report. • Diamond Claims EDI Non-Critical Errors Report. <p>Also inspected a summary of critical errors and non-critical errors for November 2004.</p>	The listings and reports tested confirmed the existence of accuracy edits in place for provider and subscriber transactions.

MACSIS - Control Objective: Accuracy of Input: Authorized transactions are accurately recorded and in the proper period.		Control Objective Has Been Met
Control Procedures:	Test Descriptions:	Test Results:
MACSIS will accurately process claim information based on pre-authorized input criteria.	Obtained listings of ODMH and ODADAS contracts. Selected 45 ODMH and 27 ODADAS contracts from the listings, and obtained an adjudicated claim listing relating to each MACSIS UPI contained on the sampled pre-authorized contracts. Of the 45 ODMH contracts selected, 37 had paid claims. All of the ODADAS contracts selected had paid claims. Recalculated the amount allowed and amount paid on each claim based on each contract and procedure code charged, and verified that the correct contracted amount was charged and paid.	The allowed ODMH amount per the adjudicated claim agreed to the contracted Medicaid rate for all 37 of the claims tested. The reimbursed amount per the claim was lower than the allowed Medicaid rate per the contracts for all 37 claims tested. The allowed ODADAS amount per the adjudicated claim agreed to or was lower than the Medicaid rate for all 27 of the claims tested. The reimbursed amount per the claim was lower than the allowed Medicaid rate per the contracts for all 27 claims tested.

MACSIS - Control Objective: Integrity of Standing Data: Changes to standing data are authorized and accurately input.		Control Objective Has Been Met
Control Procedures:	Test Descriptions:	Test Results:
Medicaid rates and information are maintained at the state level and are entered by authorized personnel.	Obtained Excel spreadsheet files of all pricing schedule (PROCP), provider contract detail (PROVD), and provider contract (PROVC) changes as well as a listing of users in user group 25 with authorized access to update these files. Used ACL to extract all changes that were made during CY 2004 from each file, and create reports of all user ids that made these changes. Compared the user listing with the ACL reports.	All users who made changes to the PROCP, PROVD, and PROVC files were members of the authorized change groups.

MACSIS - Control Objective: Integrity of Standing Data: Changes to standing data are authorized and accurately input.		Control Objective Has Been Met
Control Procedures:	Test Descriptions:	Test Results:
Procedure codes are updated by authorized personnel only.	Obtained a file of all the Procedure Code (PROCD) changes. Used ACL to extract all changes that were made during 2004 and create a report of all user IDs that made these changes. Compared the group access listing with the ACL report.	Review of the file indicated there were no changes made to the PROCD file during 2004, thus the control could not be tested.

MACSIS - Control Objective: Completeness and Accuracy of Update: Updates, modifications, and/or additions to information already on the application's files or database are accurately entered.		Control Objective Has Been Met
Control Procedures:	Test Descriptions:	Test Results:
Changes to client Medicaid eligibility are verified for completeness and accuracy.	Inspected the MHPROD AIX Production System Transactions Log Summary Control reports for 3/1/04, 3/2/04, 3/3/04, 3/27/05, 3/28/05 and 3/29/05 and example pages from the Detail Member Change reports to confirm the total number of Medicaid eligibility records transmitted from DB2 matched the total number of records updated to the Diamond 725 system. Also confirmed that changes to Medicaid eligibility were accurately updated by viewing the Detail Member Change report that reported any eligibility data changes in key fields for changed members.	All daily summary control reports tested reflected an agreement of all records transmitted to Diamond 725. The record total included "records added", "records terminated", "records changed", "records unchanged", and "records in error." The Detail Member Change report contained Medicaid information regarding records that required a change. This information included the member number, field description, current data, and new (changed) data.

MACSIS - Control Objective: Completeness and Accuracy of Update: Updates, modifications, and/or additions to information already on the application's files or database are accurately entered.		Control Objective Has Been Met
Control Procedures:	Test Descriptions:	Test Results:
Weekly procedures exist to detect and resolve discrepancies in Medicaid eligibility information from the MACSIS MEDELIG file and the ODJFS RMF file.	Inspected the comparison error report produced by MACSIS and a discrepancy report produced by ODJFS Social Security Verification System for November 2004 through March 2005 to confirm discrepancies between the Medicaid eligibility and ODJFS Recipient Master Files were being reviewed, researched, and updated.	The reports reviewed displayed possible conflicting entries. Each entry was marked appropriately by the ODMH supervisor of membership maintenance noting which entry was determined to be correct. The discrepancy reports displayed all corrections made as indicated on the comparison error reports. All comparison error reports were reviewed and reconciled to the discrepancy reports.

MACSIS - Control Objective: Completeness and Accuracy of Accumulated Data: The integrity of accumulated data is preserved.		Control Objective Has Been Met
Control Procedures:	Test Descriptions:	Test Results:
Access to accumulated claims data before adjudication is restricted to authorized personnel. Users are assigned to a security group based on the area to which they are assigned. Security flags are also assigned to each user to further define user access so that users have access only to claims associated with their group.	Inspected the MACSIS security information sheet and the access listing for users in the claims processing group.	255 users had at least WRITE access rights to the claims prior to the adjudication and finalization process. The other 146 users had, at most, Read access to this data. All users were authorized and restricted within this security group to access the claims data according to their job functions.
Modifications to historical claims are not permitted by Claims Processing management after the claims have been paid and finalized by Diamond.	Inspected a selection of claims in Diamond with a processing status of "P", which signifies the claims were paid and finalized. Attempted to alter the line item detail sections as well as the header sections of the claims to determine whether changes were permitted to be made to finalized claims.	When attempts were made to change the line item detail and header sections of the finalized claims, an error message was generated stating, "This detail record has been finalized – Cannot change."



**Auditor of State
Betty Montgomery**

88 East Broad Street
P.O. Box 1140
Columbus, Ohio 43216-1140

Telephone 614-466-4514
800-282-0370

Facsimile 614-466-4490

ODMH AND ODADAS

FRANKLIN COUNTY

CLERK'S CERTIFICATION

This is a true and correct copy of the report which is required to be filed in the Office of the Auditor of State pursuant to Section 117.26, Revised Code, and which is filed in Columbus, Ohio.

Susan Babbitt

CLERK OF THE BUREAU

**CERTIFIED
JUNE 28, 2005**