# OHIO DEPARTMENT OF MENTAL HEALTH AND ADDICTION SERVICES (OhioMHAS)

# MULTI-AGENCY COMMUNITY SERVICES INFORMATION SYSTEM (MACSIS)

# STATE REGION - ISA, FRANKLIN COUNTY

# SERVICE ORGANIZATION CONTROLS REPORT (SOC 1)

# JANUARY 1, 2014 THROUGH DECEMBER 31, 2014

Dave Yost • Auditor of State

**This Page Intentionally Left Blank**

**TABLE OF CONTENTS**

**This Page Intentionally Left Blank**

**Independent Service Auditor's Report on a Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls**

To the Ohio Department of Mental Health and Addiction Services:

*Scope*
We have examined OhioMHAS's description of the Multi-Agency Community Services Information System (MACSIS) for processing user entity transactions throughout the period January 1, 2014 to December 31, 2014 and the suitability of the design and operation effectiveness of OhioMHAS's controls to achieve the related control objectives stated in the description. Some of the servers that process the MACSIS application and certain firewall equipment are physically located in the computer room at the State of Ohio Computer Center (SOCC). The accompanying description includes only those controls and related control objectives of the OhioMHAS and did not include the controls at the SOCC related to the IT Security control objective, Physical Security. Our examination did not extend to physical security controls at the SOCC.

*Service organization's responsibilities*
In section 2, OhioMHAS has provided their assertions about the fair presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. OhioMHAS is responsible for preparing the description and for the assertions, including the completeness, accuracy, and method of presentation of the description and the assertions, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

*Service auditor's responsibilities*
Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period January 1, 2014 to December 31, 2014.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.

Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the OhioMHAS and described in OhioMHAS's assertions in section 2. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

The information in section 5 describing the user organizations is presented by the management of OhioMHAS to provide additional information and is not part of OhioMHAS's Description of controls that may be relevant to a user entity's internal control. Such information has not been subjected to the procedures applied in the examination of the Description of the controls applicable to the processing of transactions for user entities and, accordingly, we express no opinion on it.

*Inherent limitations*
Because of their nature, controls at a service organization or subservice organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization or subservice organization may become inadequate or fail.

*Opinion*
In our opinion and based on the criteria described in the OhioMHAS assertion in section 2,

a. The description fairly presents OhioMHAS's MACSIS system that was designed and implemented throughout the period January 1, 2014 to December 31, 2014.

b. The controls related to the control objectives of OhioMHAS stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period January 1, 2014 to December 31, 2014.

c. The controls of OhioMHAS that we tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period January 1, 2014 to December 31, 2014.

*Description of tests of controls*
The specific controls tested and the nature, timing, and results of those tests are listed in section 4.

*Restricted use*
This report and the description of tests of controls and results thereof in section 4 are intended solely for the information and use of OhioMHAS user entities of the MACSIS system during some or all of the period January 1, 2014 to December 31, 2014, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

**Dave Yost**
Auditor of State
Columbus, Ohio

April 10, 2015

**This Page Intentionally Left Blank**

April 10, 2015

Ohio Mental Health and Addiction Services
(OhioMHAS)
30 East Broad Street, 33rd Floor
Columbus, Ohio 43215-3430
Tel: 614 466 6680
Fax: 614 752 6474
http://www.mha.ohio.gov/

We have prepared the description of the OhioMHAS MACSIS (Multi-Agency Community Information System, for user entities of the system during some or all of the period January 1, 2014 to December 31, 2014, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. We confirm, to the best of our knowledge and belief, that

a) the description fairly presents the MACSIS system made available to user entities of the system during some or all of the period January 1, 2014 to December 31, 2014 for processing their transactions using the automated payment and management information system for mental health services. OhioMHAS use the State of Ohio Computer Center (SOCC) to house some of the servers that process the MACSIS application and certain firewall equipment. The description in section 3 of this type 2 report includes only the controls and related control objectives of OhioMHAS and excludes the controls and related control objectives of the SOCC as they relate to the IT Security Control Objective, Physical Security. The criteria we used in making this assertion were that the description

   i) presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including

      1) the classes of transactions processed.

      2) the procedures, within both automated and manual systems, by which those transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports presented to user entities of the system.

      3) the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions; this includes the correction of incorrect information and how information is transferred to the reports presented to user entities of the system.

      4) how the system captures and addresses significant events and conditions, other than transactions.

      5) the process used to prepare reports or other information provided to user entities' of the system.

      6) specified control objectives and controls designed to achieve those objectives.

      7) other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.

   ii) does not omit or distort information relevant to the scope of the MACSIS system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the MACSIS system that each individual user entity of the system and its auditor may consider important in its own particular environment.

b) the description includes relevant details of changes to the service organization's system during the period covered by the description when the description covers a period of time.

c) the controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period January 1, 2014 through December 31, 2014 to achieve those control objectives and subservice organization applied the controls contemplated in the design of OhioMHAS controls over MACSIS. The criteria we used in making this assertion were that:

   i) the risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization;

ii) the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

iii) the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Name: Rose Tolliver
Title: OhioMHAS-CIO

# SECTION 3 – DESCRIPTION OF THE SERVICE ORGANIZATION'S SYSTEM

## CONTROL OBJECTIVES AND RELATED CONTROLS

OhioMHAS control objectives and related controls are included in section 4 of this report, "Independent Service Auditor's Description of Tests of Controls and Results," to eliminate the redundancy that would result from listing them here in section 3 and repeating them in section 4. Although the control objectives and related controls are included in section 4, they are, nevertheless, an integral part of OhioMHAS's description of controls.

## OVERVIEW OF OPERATIONS

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

The MACSIS application was designed as a central benefits administration system, and is housed at the State of Ohio Computer Center (SOCC), administratively maintained from the Rhodes State Office Tower, and used by community boards and board consortiums across the state.

Community boards have access to the system through a state telecommunications network. The MACSIS software provides for eligibility checking, enrollment, service assessment, billing, and outcome monitoring functions. The system is Health Insurance Portability and Accountability Act (HIPAA) compliant and designed to meet all Ohio Department of Medicaid, and several federal reporting requirements.

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

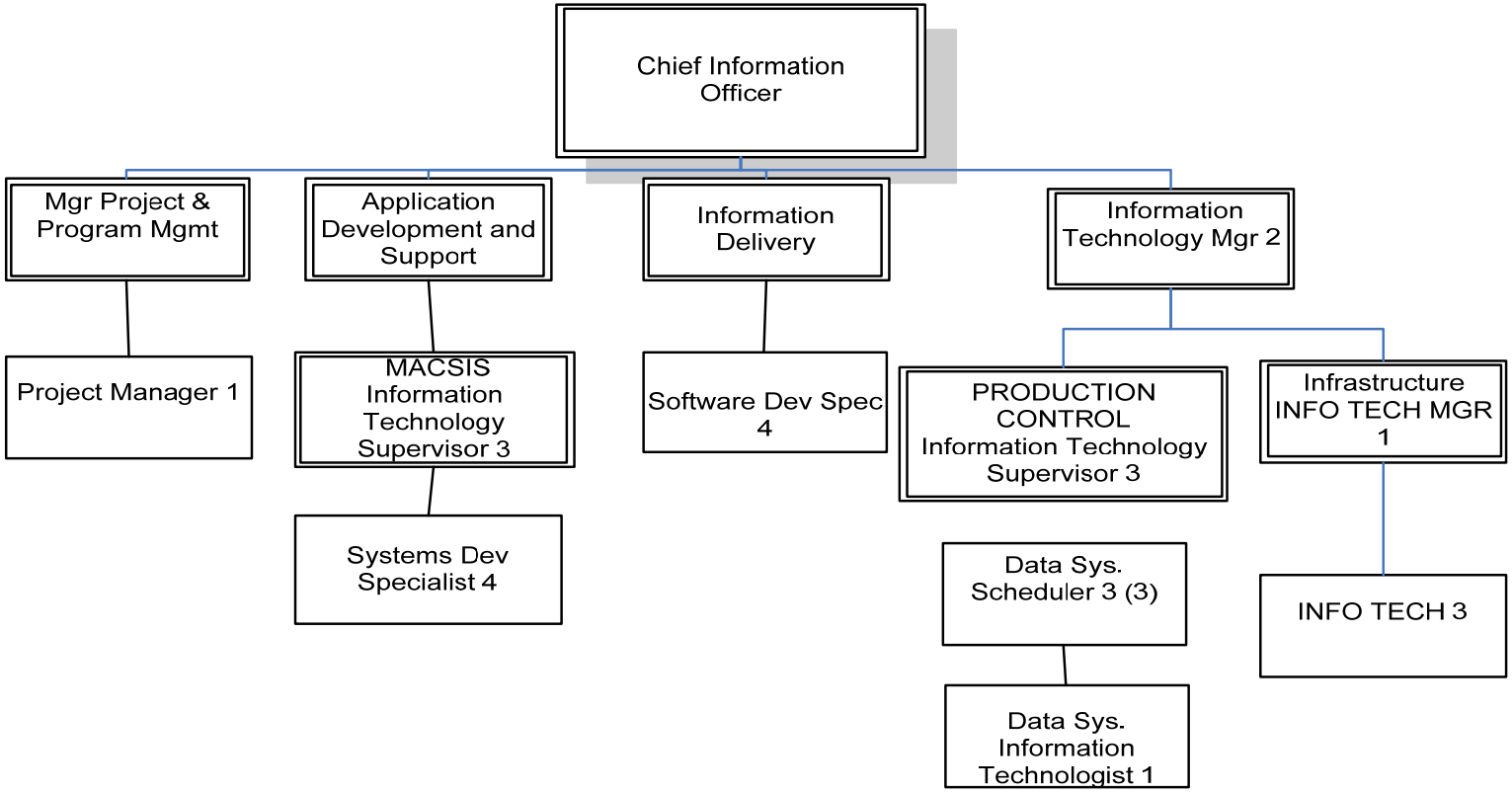
- Positions the state of Ohio and community boards to support a changing healthcare delivery environment.
- Streamlines and standardizes the flow of information from the community agencies and boards for purposes of claims submission, Center for Medicare and Medicaid Services (CMS) and State of Ohio 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 54 Alcohol, Drug, and Mental Health, (ADAMH) and community mental health and drug/alcohol boards statewide using MACSIS to process provider submitted claims. Of these 54 boards, some have grouped together to form board consortiums for their county or group of Ohio counties. These boards have contracted approximately 607 providers to perform services for clients enrolled in the MACSIS program. The boards are responsible for the adjudication and payment of non-Medicaid behavioral health claims to providers using the state supported MACSIS application. The boards collect non-Medicaid claims from the providers and pre-process them before submitting them to MACSIS to be finalized.

Medicaid-eligible claims with a date of service on and after July 1, 2012, are submitted directly from the providers to the Medicaid Information Technology System at the Ohio Department of Medicaid (ODM) for adjudication.

# OhioMHAS

## Office of Information Services (OIS)
## (MACSIS Staff Only)



## 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 the user groups noted below:

*Claims* – Comprises OhioMHAS staff that work directly with MACSIS board staff regarding communications directly related to claims, claims correction, Diamond build, etc.

*Member* – Comprises OhioMHAS staff that work directly with MACSIS board staff regarding communications directly related to member enrollment.

O*IS* – Comprises OhioMHAS staff that work directly with MACSIS board staff regarding communications directly related to OIS issues.

*Finance* – Comprises OhioMHAS staff that work directly with MACSIS board staff regarding communications directly related to finance issues (ARA's/Vouchers, payment files, etc.)

*Behavioral Health (BH) Providers* – Comprises OhioMHAS BH providers.

*MACSIS Projects and Operations Planning (POP)* – Comprises OhioMHAS staff that work directly with MACSIS board staff regarding communications directly related to projects, operation, planning issues concerning MACSIS and the MACSIS process.

*MACSIS Operations Management (MOM)* – Comprises OhioMHAS staff that work directly with MACSIS regarding communications related to MACSIS.

*All BH Stakeholders* – Comprises MACSIS MOM, MACSIS Claims, MACSIS Finance, MACSIS Members, MACSIS OIS, MACSIS POP, BH Providers, ADAMH/CMH Board, OhioMHAS Board List, OhioMHAS Provider List.

These user groups meet on an ad hoc basis to hold training sessions or to discuss changes that may result in modifications to MACSIS or related business practices. Major and minor business practice improvements and system improvements are reported to the MACSIS Operation Management (MOM) committee. The MACSIS Operation Management (MOM) committee is comprised of technical experts, managers and administrators from OhioMHAS and meets on a weekly basis.

For major system improvements or business practice issues with a significant impact on the community, issues must be formally raised through the MACSIS MOM committee. The proposed recommendations are reviewed by the committee to determine the operational impact and statewide implications within the behavioral health system. Following that review, decisions are made concerning ultimate resolution.

The IT roles and responsibilities are clearly defined through the organizational chart and job descriptions. The organizational chart is updated on an as-needed basis by the Chief Information Officer (CIO) of OhioMHAS. OhioMHAS has developed job descriptions that 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 OhioMHAS desires, a Program Enhancement Request form is submitted to the vendor. Application enhancement requests can also originate from the state and/or county board representatives via the four main user groups (Claims, Member, OIS and Finance). In addition, Statistical Analysis System (SAS) programs interface on the front and back ends of the MACSIS application to assist with claim processing and remittance. These SAS program modifications can be made by the OhioMHAS programming staff.

Additional information regarding the control environment can be found later in section 3 under the heading “General Computer Controls.”

### *Risk Assessment*

OhioMHAS does not have a formal risk management process. Working in conjunction with the IT initiatives outlined by the state of Ohio's CIO, the deputy state chief information officer, and the administrator of the Office of Statewide IT Policy, OhioMHAS actively participates in the oversight of their information technology 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 state's 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*

OhioMHAS is structured so managers report directly to the chief information officer. The key management employees of OhioMHAS are experienced with the systems and controls at OhioMHAS. The OhioMHAS chief and supervisory personnel monitor the quality of internal control performance as a routine part of their activities. To assist them in this monitoring, OhioMHAS 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.

The Office of Budget and Management (OBM) and Office of Internal Audit (OIA) audits agencies are under the Governor's oversight. The OIA personnel report to their Chief Audit Executive who reports administratively to the OBM Director and in an advisory capacity to the State Audit Committee on a quarterly basis. Internal audit work performed for the departments during calendar year 2014 was not related to the processing of MACSIS claims at OhioMHAS.

## 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 Computer Controls and Application Controls sections.

## GENERAL COMPUTER CONTROLS

### *Development and Implementation of New Applications or Systems*

The MACSIS application was supplied in 1997 by Perot Systems and was implemented and fully functioning in 1998. OhioMHAS contracts with Electronic Management Systems (EMS) as the general maintenance vendor for the Diamond 725 system.

EMS provides OhioMHAS a General Systems Design (GSD) for any new development projects. A GSD contains a step-by-step narrative of the development process required to complete the project. Each GSD also contains a proposal section specifying the estimated numbers of hours for completion and the estimated lead time.

Once OhioMHAS accepts the GSD, a Detailed System Specification (DSS) may be created. This depends on the complexity of the project and the GSD's level of detail. If produced, the DSS serves as a "road map" that guides the contractor and OhioMHAS personnel through the development process. When appropriate, additional project details are specified and addressed in the DSS. Before any programming is started, the client has an opportunity to revise the DSS.

OhioMHAS does not formally monitor the vendor's progress for system development. Periodic meetings are held with the vendor but there is no formal documentation from the vendor stating the current project status, or formal acceptance by OhioMHAS. Management's intent going forward is to require formal sign-offs prior to implementation of development projects.

During the development phase of the project, the EMS team performs unit testing and integration testing and documents the results in accordance with OIS standards. Regression testing is performed when appropriate to ensure modifications made subsequently have been properly retested. Test cases for system test is scripted and mapped back to the business requirements to ensure all requirements are met or exceeded. OIS conducts user acceptance testing after EMS completes their system test successfully. The authorization of the testing phase is recorded in the Request for Change Documentation.

All development projects are received from the vendor in the form of a new release. The vendor sends installation instructions and release notes to OhioMHAS to ensure the project is placed into production correctly.

Once the projects are tested and verified, notification is presented by the MACSIS team to the OhioMHAS stakeholders at the weekly MOM meetings. When approval is provided, OhioMHAS follows the change management process for the implementation of the project. The OIS Information Technologist moves all projects to production.

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

A structured data conversion process is followed. This process involves multiple steps to ensure data is converted appropriately. The MACSIS environment includes testing environments to validate results. Data is first copied from the production environment into a test environment. Conversion routines are executed and the results validated against production. After the systems test is completed with acceptable results, a full parallel run is executed to compare the results of the converted data to the results of normal production. All reporting and online applications are tested and validated before the converted data is moved into production.

Training for major changes is available to the county board users on an as-needed basis or at user meetings. In addition, an extensive amount of documentation including electronic format requirements, system guidelines, presentations, and reports, is available via the Web.

***Changes to Existing Applications or Hardware Systems***

MACSIS consists of the following four components:

- Pre-processor programs.
- Diamond 725 system.
- Medicaid eligibility system (supported by Ohio Department of Medicaid).
- Board financial systems (not supported by state MACSIS staff).

OhioMHAS uses the Dell 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 (these are not supported by state MACSIS staff and only a few boards have interfaces).

There are 2,682 Diamond 725 programs written in BBx and housed on multiple AIX6000 servers. Source code is copyrighted by Dell Perot Systems.

There were no upgrades to the Diamond production release environment implemented during calendar year 2014. The production version was still 8.3.1F. However, there were six changes (program modifications) to the Diamond production environment implemented during calendar year 2014. OhioMHAS installed the six program enhancements on the Diamond 725 core system during the audit period.

OhioMHAS made 24 (Statistical Analysis System) SAS or non-Diamond program modifications during calendar year 2014.

OhioMHAS maintains a software maintenance agreement with EMS for the MACSIS application residing on the AIX servers. This agreement allows for general maintenance and software warranties.

When upgrades are provided, the vendor provides release notes to OhioMHAS 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 application. If OhioMHAS requests a change to the processing, reporting or functionality a *program enhancement* must be conducted by the vendor. 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 the vendor, and logged at OhioMHAS.

Diamond Program Enhancements

Proposals for major Diamond enhancements are initially presented to the MACSIS MOM committee to consider budget constraints and project validity. Approval from OhioMHAS program change management is required on all program enhancement forms before submission to the vendor for further processing.

Once the vendor receives the request, the vendor 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 (CIO and Deputy Director of Administrative Services), and/or the Behavioral Health Operations Committee (for issues that impact statewide behavioral health operations or policies only) for their view on the proposed change. The OhioMHAS CIO approves the final proposal. Original program enhancement forms are logged and maintained by OhioMHAS to monitor the status of all program change projects requested of the vendor.

Testing of enhancements is performed in the various areas of Office of Information Services (i.e. Claims, Membership, and Accounts Payable) by the OIS Information Technology section supervisors. Each OIS section supervisor is responsible for testing the relevant portions of the MACSIS application for their section. This testing phase includes running production data in parallel test mode for one week when enhancements are requested.

** There were no Diamond program enhancements made to the MACSIS production environment during calendar year 2014.

Diamond Program Modifications

Proposals for Diamond program modifications originate from the state or county board representatives relating to an error in the processing or reporting or a problem with the design of the application. If a program modification is required, the Change Management process within OhioMHAS is followed to track the implementation of that modification. The issues process log is centrally maintained by OhioMHAS to report and track the progress and status of all MACSIS program modifications. The log contains the date the issues were reported, affected programs, as well as dates indicating when the modification was received, tested, and moved to the live environment. The log entry is sent to the vendor by the supervisor or project manager who discovered the problem. The vendor support personnel logs and tracks the problem resolution internally.

The vendor decides on the resolution strategy and assigns programmers to complete the task. Once the modification is completed, the vendor sends the program fix to OhioMHAS for testing and implementation, and the issue process log is updated with the date the fix was received.

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. The Diamond Test Libraries Log is updated once testing of Diamond program modifications has been successfully completed by MACSIS personnel.

Once the program changes are tested and verified, notification is presented at the bi-weekly MOM meetings. Following the OhioMHAS change management process, the OIS Information Technology supervisor approves and then initiates the migration of all changes from the test environment into production. The supervisor updates the issues process log with the appropriate date.

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 modified programs into the live environment.

** There were six Diamond program modifications made to the MACSIS production environment during calendar year 2014.

Diamond Program Enhancements and Modifications

All large enhancements and modifications are received from the vendor in the form of a new release. The vendor sends installation instructions and release notes to OhioMHAS prior to each new release to ensure the upgrade is placed into production correctly utilizing the OhioMHAS change management process.

MACSIS documentation is updated to reflect the program change made. MACSIS technical notes are available on the Internet to the board and county users to notify them of any minor changes to the MACSIS system. Minutes are distributed to POP members that include topics discussed, project updates, user group updates, board global issues and plans for the next meeting. Open and closed issues logs are also maintained for statewide issues reported.

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.

The vendor provides detailed summaries of any changes made to the MACSIS application and sent to OhioMHAS.

Non-Diamond (SAS) Program Modifications

To assist the MACSIS claims processing executed by the Diamond software, front and back-end processing also occurs by related SAS programs used for MACSIS claims pre-processing or remittance. OhioMHAS tracked all SAS program modifications for calendar year 2014.

OhioMHAS utilizes a formal change management process that requires successful testing of SAS program changes prior to implementation. A request for change form (RFC) must be submitted and approved prior to making changes to the production environment.

Access to the SAS production libraries is restricted to authorized OhioMHAS personnel. To allow a user to update or modify SAS programs, the user must have an AIX (specific brand of UNIX) account on the production server, and a specified SAS directory in their user profile.

** There were 24 non-Diamond (SAS) program modifications made by OhioMHAS in calendar year 2014.

***IT Security***

Security Management

User access to the MACSIS application is restricted and 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 group access and capabilities should be granted to the user at the application level.

Confidentiality of data requirements have been appropriately considered by MACSIS management, documented, and distributed to users for their sign-off. Initial-level access to the MACSIS application is appropriately defined in the AIX operating system and authorized by appropriate OhioMHAS personnel. AIX security is administered by OIT security personnel.

A reconciliation of users' Diamond 725 access is conducted by the OIS at OhioMHAS on an annual basis to confirm that all users with access to the MACSIS application are appropriate. Each year, OIS distributes a list of all users to their respective county boards to validate their need for access to the MACSIS application. However, the periodic access reconciliation does not validate the level of access to the MACSIS programs and data assigned to each user.

OhioMHAS has procedures to address the termination or transfer of employees and effect the necessary changes in their access to computer systems. An Exit Interview Checklist is completed by OhioMHAS for employees who are separating employment or transferring to another division.

A "Guideline Pertaining to MACSIS" outlines the state and board's communication responsibilities regarding MACSIS system access.

Security violation reports are captured and e-mailed to the Customer Services section 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 alerts are enabled through AIX to monitor logon security violations and will automatically e-mail the OIT Infrastructure Services Division (ISD) Operating System Services and Support security management group (OSSS). OSSS will send a failed login report to the OhioMHAS OIS Information Technology supervisor when the failed logon threshold is exceeded.

All OhioMHAS PCs are equipped with anti-virus software that is scheduled for weekly automatic updates. All incoming e-mails are also scanned.

Policies and procedures relating to computer security and use have been issued by OhioMHAS to address specific security issues such as personal computer usage, electronic mail and security, physical access, password and user IDs, and remote access. These policies cover personal computer usage, World Wide Web activities, e-mail usage, and password/user ID requirements. HIPAA security-related policies are also in place. Policies are available to MACSIS personnel through the OhioMHAS intranet sites.

The OhioMHAS 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 OhioMHAS and operating subsidiaries.

IT Access

An AIX server is used by MACSIS to extract the latest Medicaid eligibility information from Ohio Department of Medicaid and update the Diamond software. For a user to logon to the server, a unique user ID and password are required. Community users can use telnet software, which requires a unique user ID and password to remotely login to this AIX server.

System password controls have been established for the AIX system on the production servers that process 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.

AIX password parameters require a minimum number of non-alphabetic and special characters. Each MACSIS application user must login to the MACSIS production AIX server with their unique AIX user ID and password to prevent unauthorized access to transactions. Once logged into the production server, all users may access the main menu of the Diamond 725 application by entering a unique user Diamond 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 five different AIX servers and there are two support services AIX servers. These servers house the development, testing, data warehouse, transferring, reporting 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 ISD network via the Internet, a user enters a SecureID code and a personal identification number (PIN). The SecureID code is generated by a SecureID token authorized to and carried by the user. The unique SecureID code is generated every 60 seconds by a computer chip inside the token. To initiate the login process, the user must enter the SecureID code displayed on the token along with a unique PIN.

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 AIX user IDs. Also upon authentication, the system ensures an encrypted path between the remote device (SecureID card) and ISD to prevent the information from being read and interpreted during transmission.

AIX administrative 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 OSSS group also maintains an encrypted system security password file. In the AIX 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

OhioMHAS's Password and User ID Policy includes the following guidelines for password administration:

- Passwords must contain at least one alphabetic and one non-alphabetic character.
- Passwords must be a minimum number of characters in length.
- Passwords must be changed according to a predefined password lifetime.
- Passwords cannot be reused for at least one calendar year.
- Accounts are locked after a predefined number of unsuccessful attempts to enter a password.
- Passwords are tested at least once per calendar year based on a risk assessment.

Diamond application passwords do not adhere to the standards established in the Password and User ID Policy. These parameters are less restrictive than those in the policy guidelines described above. Password parameters have been hard coded into the Diamond 725 system. However, all users must have an AIX logon to access Diamond, which is the only application available to users on the server. A failure at the AIX level would prohibit access to Diamond.

Network Firewalls and Physical Security

Two of the MACSIS servers, one functioning as the test and one HIPAA-compliant production server, are located at the State Office Tower (SOT). The remaining five servers, functioning as the HIPAA compliant production environment, web service, data warehouse, and other development environments are located at the SOCC.

Access to the production servers on the DAS wide-area network (WAN) is protected from unauthorized outside exposure by filtering routers and firewalls that are maintained on WAN, as well as a firewall for the OhioMHAS local area network environment where the MACSIS servers reside. Controls related to physical security, to the filtering routers and firewalls, and to the environment of the computer rooms, are performed by DAS personnel of the SOT and SOCC, and are not the responsibility of OhioMHAS management.

Data traffic coming into the OhioMHAS network must pass through a firewall that provides protection from unauthorized Internet (IP) traffic attempting to enter the OhioMHAS network. Unauthorized OhioMHAS network traffic is monitored by network personnel to identify key intrusion events in a timely manner.

Logical access to the firewall rules is restricted to appropriate personnel. Modifications to the OhioMHAS firewall rules are documented by Network Services to provide support for all changes made.

***IT Operations***

MACSIS batch production processes are documented, scheduled, and maintained on an ongoing basis. Each morning, a file is sent from the Ohio Department of Medicaid with the latest Medicaid eligibility information. The MACSIS servers and data files are updated with these Medicaid eligibility updates through a nightly batch process. The MACSIS production batch jobs are pre-scheduled through the BMC Control-M scheduling software or manually initiated and documented on the Update Daily Run Log by the OhioMHAS 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 OIS Production Control and retained for approximately two years. OhioMHAS also runs weekly batch jobs related to MACSIS processing. The batch jobs produce reports to summarize the total claims and dollar amounts for the county boards, and also run to post the reimbursement payments to the county boards. A policy relating to data retention has been issued by OhioMHAS to address specific data retention requirements.

The International Business Machines (IBM) system software upgrades and releases are selected based on critical fixes and enhancements included in 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. Additionally, a system backup is performed once a month on each system and/or when a major change is made, and can be used to recover a system to a previous state.

IBM Tivoli Storage Manager, TSM, is used to schedule and maintain server backup and recovery. Daily incremental backups on all MACSIS servers are performed automatically. Completion of the backups is documented on the daily backup log. Files backed up by the job are contained in the Query Filespace Command Output Report. The data is stored in an EMC VNX Storage System which contains hard disks, not magnetic tapes, to store backup data. TSM is configured to help ensure that any/all files can be restored to any date/time within 30 days. 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 60 days. A log of the TSM incremental backups is created with each run and retained for a period of seven days. Although the backups are performed by OSSS, determination of successful backup is the responsibility of MACSIS management.

Redundant off-site incremental system backups are performed automatically on a daily basis. For servers located at each location (SOCC and SOT), backups are stored at the alternate server location. The Tivoli Storage Manager (TSM) job schedule is used to indicate the status and frequency of the scheduled jobs. The administrative task list contains the start and end time for each job as well as a completion status. Each day, a job is submitted 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 local stored volumes to the off-site storage (i.e. the SOT volumes contain backup files for SOCC servers, and the SOCC volumes 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 for publicly-funded behavioral health services and is accessed by community boards and board consortiums across the state. Community boards have access to the system through a state telecommunication network. The software provides for eligibility checking, enrollment, service assessment, billing, and outcome monitoring functions. The system is HIPAA compliant and designed to meet ODM and federal reporting requirements.

*Overview*

MACSIS is an information system that allows OhioMHAS, and their local boards to manage, measure, and monitor the behavioral health service utilization of state and local public funds. MACSIS consists of the following components:

1. The Provider Number Validation scripts electronic transfer of claims data between the county boards and State, between the State's SFTP server and the production server.

2. The Diamond 725 system adjudication process includes membership management, provider contract management, the new FIFO claims adjudication processing, and accounts payable/remittance advice functionality.

3. The Medicaid eligibility system updates the Diamond system daily to manage non-Medicaid plan assignments and eligibility periods.

4. The board financial systems interface to receive accounts payable data from Diamond 725.

*Claim Submission Process*

The submission process refers to the flow of claims data submitted by providers (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 provider'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 in MACSIS and for instructing providers on how to verify eligibility. MACSIS receives automatic nightly updates of eligibility information from ODM's Medicaid Information Technology System (MITS).

2. Electronic Transmission of Claims

   This step involves the process of a provider submitting claims electronically to their designated board for forwarding to MACSIS. Providers 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 non-Medicaid (i.e. other publicly-funded) programs.

3. Board-Level Claim Adjudication and Remittance

   Each board transfers incoming provider claim files to MACSIS, which is used to adjudicate claims for payment according to the contracts and agreements the boards have established with their providers. 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 provider contract or agreement. In all cases, a remittance report generated by the board accompanies payment.

*Electronic Data Interchange (EDI) System*

The EDI system completes the pre-scrubbing process that included the HIPAA compliance validation and provider information validation. In addition, all claim files from the boards are SFTPed (secure file transfer protocol) to the state SFTP server. Then, the state SFTP server sends the files to the MACIS production server. The Diamond 725 system processes the board claim files according to the SFTP stamp, which is first in first out (FIFO).

The EDI process allows MACSIS to receive electronic claims, process the electronic claims using standard Diamond adjudication logic, and creates electronic Remittance Advice files. The module is designed so that all existing Diamond functionality will work as normal.

*Provider and Client Enrollment*

County boards are responsible for managing Medicaid and non-Medicaid contracts with providers and for deciding upon non-Medicaid fees for services (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 receiving non-Medicaid services who are served with public funds (federal, state, or local levy) must be enrolled in MACSIS.

*Submitting Claims*

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.

When boards enroll contracted providers in MACSIS, the providers are assigned provider IDs called UPIs (Unique Provider Identifier). Providers can be a person, place, or organizational group. A valid UPI must be submitted on each claim prior to processing.

National Provider Identifiers (NPI) are unique health provider identifiers designed to be lifelong numbers used to distinguish individual practitioners

or provider organizations on standard electronic health care transactions. For MACSIS, the provider's Type-2 NPI is cross-walked to the UPI number in Diamond to adjudicate claims.

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.

Professional behavioral health service claims must be submitted electronically to the boards in a HIPAA-compliant format, as currently required under HIPAA. Inpatient facility psychiatric claims are not currently being electronically submitted or processed through the MACSIS system.

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.

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.

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. Responses 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.

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 processing. The files are swept out of suspense three times a day and run through the Pre-Processing Validation Program and then sorted for adjudication by the FIFO program.

*Pre-Processing Validation Program*

FIFO will run programs against files in the input directory and move them to the correct location for adjudication.

*Duplicate Testing*

Edit checks are also performed by Diamond 725 during claims EDI processing to help identify and deny duplicate claims. The status of processed claims (allowed, denied, etc.) is detailed in the Post-EDI Transaction Set Job Log and the ASC report. Any claim with the same procedure code and modifier combination will be denied, if the claim is for the same provider, date of service and client. Additionally, benefit rules are in place that limit and deny certain services when certain services are being billed or the daily eligibility limits for adults and children are reached.

*Pre-Adjudication Processing*

Prior to MACSIS adjudication, UNIX scripts are executed twice a day (11:30 AM and 2:30 PM) to collect files from board SFTP directories and validate the provider ID in the file name; only accepting the files from the approved providers according to the ANSI version approval status. Files with unapproved providers are rejected. An email is sent to each board/consortia indicating the file name of any rejected file so the provider can make corrections and resubmit later. All the valid files are SFTP'd to the correct location for adjudication in the same order as they are received at the SFTP server, then moved out of SFTP directories.

*Claims EDI Processing*

All valid records are deposited by a Pre-processing Validation Program into a directory on the Diamond system for each submitter. The FIFO process is run for each board on a daily basis. 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. Edit errors are recorded on either the Diamond Claims EDI Critical Errors Report or the Diamond Claims EDI Non-Critical Errors Report. The boards authorize the posting of the Claims EDI process.

*MACSIS Processing*

MACSIS will accurately process claim information based on fee schedule rates loaded into MACSIS. 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.

All reports 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 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.

Non-Medicaid service rates, procedure code, and pricing information are maintained in the Diamond application and entered by authorized personnel. Procedure codes are updated by authorized personnel only. These rates and information are contained on various data files such as the Pricing Schedule (PROCP), Provider Contract Detail (PROVD), Provider Contract (PROVC), and Procedure Code (PROCD). Changes to these files are maintained in Diamond.

*Medicaid Eligibility*

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. ODM maintains Medicaid eligibility data in the Recipient Master File (RMF). Each morning, MACSIS accesses the RMF file and imports 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 SFTP 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 ODM RMF file. Exception reports are produced to notify the Membership Maintenance Group of discrepancies between the MEDELIG and RMF files. The Membership Maintenance Group then researches and resolves the exception report items.

*Claims Resubmission*

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 (non-recurring, claim specific info) 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. 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. Modifications to historical claims are not permitted by Claims Processing management after the claims have been finalized by Diamond.

**MACSIS and MITS Claims Processing Transition Background**

Beginning in state fiscal year 2013 (July 1, 2012), the state's share of these Medicaid claims was funded by the Ohio Department of Medicaid (ODM), which is Ohio's single state Medicaid agency. The state resources to support Medicaid claims were appropriated in the ODM budget along with most of the Medicaid programs. As a result, the MITS claims payment system was modified to enable that department to pay behavioral health providers directly for these claims.

For all Medicaid claims with a date of service July 1, 2012 and later, providers will submit Medicaid claims directly to MITS. In addition,

- Medicaid claims MUST go directly into MITS. Boards cannot require providers to use MACSIS for Medicaid claims.
- This change is based on date of service, so if a Medicaid claim with an earlier date of service is submitted after July 1, 2012, that claim must be submitted through MACSIS for adjudication.
- If a consumer is Medicaid eligible and is seeking and receiving services prior to July 1, 2012, the board will continue to be responsible for enrollment of the client in MACSIS. Boards will only be responsible for enrollments in MACSIS for a consumer seeking and receiving

services with a start date after July 1, 2012, in the instance that the board is financially responsible for that consumer's services (e.g., a Medicaid consumer receiving non-Medicaid reimbursable services or a non-Medicaid consumer). With that said, the state will facilitate the updating of Medicaid information to boards in order to inform payment of related non-Medicaid services and manage overall behavioral health community planning. Further guidance on board and provider responsibilities versus the state's role in eligibility will be available after subsequent discussions.

- Medicaid retroactive claiming will continue so boards can recoup reimbursement from Medicaid as appropriate in situations where a service is rendered on a date when the person was later determined to be Medicaid eligible. Claims for services with dates of service prior to July 1, 2012, would still be billed through MACSIS even if the eligibility is established after July 1 and then retroactively covers prior dates of service.

**** No Medicaid claims were processed through MACSIS during calendar year 2014.**

**Non-Medicaid Claims Approach**

MACSIS remains available to process non-Medicaid claims until a replacement approach for non-Medicaid claims payment and data exchange is identified and implemented with the ADAMH boards.

## COMPLEMENTARY USER ENTITY CONTROLS

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

### *General Computer Control Procedures*

- 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 of 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 in compliance with established data retention schedules.

***MACSIS Application Control Procedures***

- 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.
- After posting claims, user boards should review the Process EDI (PREDI) post report and resolve the error messages.
- User boards should review all remittance advice reports (for Non-Medicaid [835]) 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.
- Periodic reviews of the non-Medicaid contract rate data should be performed at each board to verify that contract activity is authorized and valid.
- 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.
- 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" and limited 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 entity controls presented above do not represent a comprehensive set of all the controls that should be employed by user entities. Other controls may be required at user entities.

# SECTION 4 - INDEPENDENT SERVICE AUDITOR'S DESCRIPTION OF TESTS OF CONTROLS AND RESULTS

*This section is intended to provide interested parties with information sufficient to obtain an understanding of those aspects of the MACSIS system that may be relevant to user entity'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 OhioMHAS and procedures performed at user entities that utilize MACSIS.*

*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 COMPUTER CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS

### *Development of New Applications and Systems*

No new MACSIS application development or implementations occurred during calendar year 2014.

### *Changes to Existing Applications and Systems*

| **Changes to Existing Applications and Systems -** *Control Objective:*<br>**Change Requests** - Requests for application program changes or system upgrades should be appropriately considered and processed. | | ***Control Objective Has Been Met*** |
|---|---|---|
| *Control Procedures:* | *Test Descriptions:* | *Test Results:* |
| **Diamond Changes**<br>MHAS maintained software maintenance agreements for the MACSIS application residing on the AIX servers. | Inspected the SFY14 and SFY15 software support agreements and proof of contract payments. | No exceptions noted. |
| **Diamond Changes**<br>All Diamond programs moved into the live environment by MACSIS personnel are logged by the Request for Change (RFC) documentation. The document contains the date the issues were reported and implemented, as well as key programs affected by the change. | From a listing of all Diamond programs with the last change date during the audit period, sampled 2 of 6 changes and inspected changes requested for change documentation, descriptions, and approvals of the changes contained within a new release. | No exceptions noted. |

| **Changes to Existing Applications and Systems -** *Control Objective:*<br>**Change Requests** - Requests for application program changes or system upgrades should be appropriately considered and processed. | | ***Control Objective Has Been Met*** |
|---|---|---|
| *Control Procedures:* | *Test Descriptions:* | *Test Results:* |
| **SAS Changes**<br>OhioMHAS has a policy in place for MACSIS program modifications. Changes made to the MACSIS SAS programs are documented and maintained to report and track the status of program modifications. | Inspected the MACSIS Request for Change Policy and RFC Manual to confirm procedures were in place for MACSIS SAS program modifications.<br><br>Inspected the log of OhioMHAS SAS program changes and SAS RFC listing to verify the status of program changes was being reported and tracked.<br><br>From the listings of 24 SAS program changes, selected 5 changes and inspected documentation of the request, approval, and testing. | No exceptions noted. |

| **Changes to Existing Applications and Systems -** *Control Objective:*<br>**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:* |
| **Diamond Changes**<br>Access to the Diamond 725 test libraries is restricted to authorized personnel within Information Services. | Inspected the AIX user ID listing of individuals with access to the test source and object libraries on the test server. | No exceptions noted. |
| **Diamond Changes**<br>Testing of program changes is performed by the MACSIS personnel prior to migration to production. | Inspected the CY14 Diamond Production Library Log for 2 of the 6 changes and confirmed that each sampled change had a corresponding test script created before the program change was moved to production. | No exceptions noted. |

| **Changes to Existing Applications and Systems -** *Control Objective:*<br>**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:* |
| **SAS Changes**<br>The testing of OhioMHAS SAS changes is approved on the RFC documentation. | From the listing of OhioMHAS SAS program changes, selected 5 of 24 changes and inspected the RFC documentation for evidence of testing approval. | No exceptions noted. |

| **Changes to Existing Applications and Systems -** *Control Objective:*<br>**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:* |
| **Diamond Changes**<br>Access to the Diamond 725 production libraries is restricted to authorized personnel. | Inspected the Diamond AIX admin 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, inspected the group and group members with access to su to the Diamond account to confirm authorized access to production libraries. | No exceptions noted. |
| **Diamond Changes**<br>All Diamond programs moved into the live environment by MACSIS personnel are logged by the Diamond production libraries. | Inspected the MACSIS MHHIPAA Diamond production programs change log for CY14 to confirm the log was updated with the CY14 date the Diamond program modifications were moved to the live environment. | No exceptions noted. |
| **SAS Changes**<br>Access to the SAS production libraries is restricted to authorized personnel. | Inspected the Diamond AIX user profiles for individuals with access to update the SAS programs. | No exceptions noted. |

| **Changes to Existing Applications and Systems -** *Control Objective:*<br>**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. | | ***Control Objective Has Been Met*** |
|---|---|---|
| *Control Procedures:* | *Test Descriptions:* | *Test Results:* |
| MACSIS documentation is updated to reflect the Diamond and SAS program change made. | Sampled 2 of 6 Diamond changes that occurred during CY14 and inspected the related program change documentation, RFC forms, for evidence the changes were documented.<br><br>Inspected the OhioMHAS SAS Program Change log for descriptions of changes made to the SAS programs. From a population of 24 program changes, sampled 5 changes and inspected related program documentation for evidence the changes were documented within the RFC. | No exceptions noted. |

***IT Security***

| **IT Security -** *Control Objective:*<br>**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 restricted and authorized via use of MACSIS access request forms. | For 3 of 12 AIX users added during CY2014 that were granted MACSIS access, inspected the corresponding MACSIS access request forms for staff signature, supervisor signature, and OIS personnel signature. | No exceptions noted. |
| Confidentiality of data requirements have been considered by MACSIS management, documented, and distributed to users. | For 3 of the 12 AIX users added during CY 2014 that were granted MACSIS access, inspected the disclosure of information forms for a user signature. | No exceptions noted. |
| AIX-level access is restricted, and authorized via use of TCP/IP account request forms. | For 3 of the 12 AIX users added during CY 2014, inspected the corresponding TCP/IP access request forms for access rights and supervisory approval. | No exceptions noted. |
| A reconciliation of users' Diamond 725 access is conducted by the OhioMHAS OIS on an annual basis to confirm that all users with access to the MACSIS application are appropriate. | Inspected confirmation documentation for 6 of the 36 counties/boards and compared any changes requested on the confirmation to the AIX file and the MACSIS system administrator access grouping to confirm that changes in access rights were updated accordingly. | No exceptions noted. |
| Detection control alerts are enabled to monitor logon security violations and will automatically e-mail the OIT ISD OSSS Group (security management) when logon attempt thresholds are exceeded. | Inspected 21 of 205 AIX failed logon attempt e-mail notifications of security violations that occurred during CY14 for evidence that notification was sent to appropriate personnel for follow up when the failed logon attempt threshold was exceeded. | No exceptions noted. |
| Policies and procedures relating to computer security and use have been issued by MHAS to address specific security issues such as personal computer usage, electronic mail and security, physical access, password and user IDs, and remote access. | Inspected the MHAS IT policies and procedures for inclusion of specific computer usage and security topics. | No exceptions noted. |

| **IT Security -** *Control Objective:*<br>**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:* |
| An Exit Interview Checklist is completed by MHAS for employees who are separating employment or transferring to another division. | Inspected a listing of MHAS employee departures during the audit period. From the listing of 42, sampled 6 users and obtained the corresponding Exit Interview checklists for each of the separated employees.<br><br>Confirmed the sampled terminated employees had their network, AIX, and Diamond accounts removed or disabled. | No exceptions noted. |
| MHAS has procedures to address the termination or transfer of employees and effect the necessary changes in their access to computer systems. | Inspected the MHAS termination procedures to confirm specific termination procedures have been addressed including the notification of OIS. | No exceptions noted. |

| **IT Security -** *Control Objective:*<br>**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 accounts 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 to confirm passwords required the following parameters:<br>• Minimum length.<br>• Minimum number of alpha, numeric, and special characters.<br>• Maximum time period before password expires.<br>• Minimum length of time until a password can be reused. | No exceptions noted. |

| **IT Security -** *Control Objective:*<br>**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 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 to confirm parameters were in place to lock accounts after a maximum number of failed sign-on attempts. | No exceptions noted. |
| Data traffic coming into the OhioMHAS network must pass through a firewall that provides protection from unauthorized Internet (IP) traffic attempting to enter the OhioMHAS network. | Inspected the OhioMHAS/OIT network connectivity diagram.<br><br>Inspected the firewall rules for evidence of a network infrastructure, which included the use of firewalls that restricted unauthorized IP traffic.<br><br>Inspected example OhioMHAS dedicated environment firewall violation logs for two days of each month from July 2014 through December 2014. | No exceptions noted. |
| Modifications to the OhioMHAS firewall rules are documented by Network Services to provide support for all changes made. | Inspected the OIT Unified Network Services network change management process.<br><br>Inspected the Policy Install Journals from January 2014 through December 2014 for the OhioMHAS dedicated environment firewalls to confirm firewall rule change documentation. | No exceptions noted. |
| Logical access to the firewall rules is restricted to appropriate personnel. | Inspected the OhioMHAS dedicated environment Firewall Administrator's permissions and confirmed access rights were appropriate. | No exceptions noted. |

| **IT Security -** *Control Objective:*<br>**Application Level Access Controls -** 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. | | ***Control Objective Has Been Met*** |
|---|---|---|
| *Control Procedures:* | *Test Descriptions:* | *Test Results:* |
| Each MACSIS application user must have a user ID and password to prevent unauthorized access to transactions. | Attempted to access the MACSIS production application with the following test scenarios:<br>• Enter a valid user ID and no password.<br>• Enter a valid user ID and a password.<br>• Do not enter a user ID and password.<br>• Enter a valid user ID and an invalid password. | No exceptions noted. |
| The MACSIS application incorporates security groups to define and segregate the use of transactions for all users. | In a test environment, created three user accounts, each defined to a different security group and related transactions. Attempted to execute transactions not defined within that security group. For example, group A is only defined to execute transaction 1; a group A user should not be able to execute transaction 2, 3, or 4. | No exceptions noted. |
| MACSIS application access is assigned based on the security groups requested on the MACSIS Account Request Forms. | For 3 of the 12 new users granted MACSIS access during CY2014, compared the MACSIS access request forms to access granted in the system. | No exceptions noted. |

| **IT Security -** *Control Objective:*<br>**System Software and Utilities Access Controls -** Use of master passwords, powerful utilities and system manager facilities should be adequately controlled | | ***Control Objective Has Been Met*** |
|---|---|---|
| *Control Procedures:* | *Test Descriptions:* | *Test Results:* |
| Access to alter and maintain sensitive system software and utilities is limited to authorized personnel and is restricted and monitored. | Inspected the AIX Login/Logout Activity Logs and the AIX Switch User (SU) Logs for the months of 10/14, 11/14, and 12/14, to confirm only authorized personnel logged into the system as root.<br><br>In addition, inspected sample e-mail notifications of successful and failed connection attempts to switch user (su) to root to confirm an alert was sent to management when successful or failed su to root attempts were made. | No exceptions noted. |
| Access to the encrypted AIX security password file is restricted to the network security personnel. | Inspected the access privileges to the encrypted AIX password file to confirm authorized access | No exceptions noted. |
| Access to Diamond system administrator privileges is restricted to authorized IT personnel. | Inspected the Key Word Security Groups listing and the System Administration Access grouping to confirm authorized access. | No exceptions noted. |

| **IT Security -** *Control Objective:*<br>**Physical Security** - Computer facilities and data should have appropriate physical access restrictions and be properly protected from environmental dangers. | | ***Control Objective Has Been Met*** |
|---|---|---|
| *Control Procedures:* | *Test Descriptions:* | *Test Results:* |
| The computer room and data processing facilities and equipment at the SOT are protected by environmental and physical access controls. | Performed a walkthrough of the seventh floor server room at the SOT. (Containing a test and HIPAA-compliant production server)<br><br>In addition, inspected the door access report for the SOT 7th floor OIT Network Services computer room to confirm access was appropriate for user job responsibilities. | No exceptions noted. |

***IT Operations***

| **IT Operations -** *Control Objective:*<br>**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 daily and weekly reports on an ongoing basis. | Inspected 22 Daily Run Logs for evidence that batch jobs were documented, scheduled, and maintained on an ongoing basis.<br><br>Inspected 7 of 52 for each of the two weekly claims reports for evidence of successful completion of the check post and voucher reimbursement jobs. | No exceptions noted. |
| A policy relating to data retention has been issued by MHAS to address specific data retention requirements. | Inspected the MHAS OIS policy section, Forms and Records Management, as well as the Ohio Revised Code referenced in the policy. | No exceptions noted. |

| **IT Operations -** *Control Objective:*<br>**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:* |
| Daily incremental backups on all MACSIS servers are performed automatically. Completion of the backups is documented on the daily backup log. Files backed up by the job are contained in the Query Filespace Command Output Report. | Inspected the daily backup logs for the week of 2/12/15 through 2/18/15 for evidence the incremental backups were performed daily.<br><br>Inspected the Query Filespace Command Output Report showing all the production backup files in the local virtual backup environment at the SOCC. | No exceptions noted. |

| **IT Operations -** *Control Objective:*<br>**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:* |
| Redundant off-site incremental system backups are performed automatically on a daily basis. For servers located at each location (SOCC and SOT), backups are stored at the alternate server location. | Inspected the Tivoli Storage Manager (TSM) job schedule script and related status information for the daily off-site dual server backups.<br><br>Also, inspected the status of administrative backup tasks for the weeks of 1/19/15 through 2/18/15 for indication of successful completion. | No exceptions noted. |

# APPLICATION CONTROLS PLACED IN OPERATION AND TESTS OF OPERATING EFFECTIVENESS

***MACSIS***

| **MACSIS - *Control Objective:***<br>**Authorization:** Information entered into MACSIS represents valid data approved by the entity's management. | | ***Control Objective Has Been Met*** |
|---|---|---|
| *Control Procedures:* | *Test Descriptions:* | *Test Results:* |
| Only authorized claim data is submitted for further processing. | Inspected the MACSIS Member Field Descriptions listing to confirm the Unique Client Identifier (UCI) must be utilized when submitting a claim for payment or credit.<br><br>Inspected the PREDI error codes listing, as well as a summary of critical errors to confirm edits were in place to require valid UCI's.<br><br>Inspected the MACSIS837 Professional Claim Informational Guide to confirm a valid UPI must be submitted on each claim prior to processing. Also inspected the PREDI error codes listing to confirm edits were in place to require valid universal provider IDs - state (UPI's).<br><br>Inspected the claims EDI process flow for 837P in MHHIPPA to confirm it contained steps to validate authorized claims being submitted from boards. | No exceptions noted. |

| **MACSIS - *Control Objective:***<br>**Authorization:** Information entered into MACSIS represents valid data approved by the entity's management. | | ***Control Objective Has Been Met*** |
|---|---|---|
| *Control Procedures:* | *Test Descriptions:* | *Test Results:* |
| Fatal error edits are in place within the Diamond application to ensure valid data is submitted for processing. | Inspected the PREDI Error Codes listing for the period 1/1/14 to 12/31/14. Selected all six of the operational fatal errors from the listing. Confirmed the edits were functioning in the test region and obtained screen prints of the error messages:<br>1. OPE001 – Requires a valid date of service.<br>2. OPE005 – Requires the subscriber number to be populated.<br>3. OPE010 – Requires a subscriber name to match the subscriber number.<br>4. OPE015 – Requires a valid subscriber number.<br>5. OPE018 – Requires modifiers for the 837 file to be populated.<br>6. OPE630 – Requires modifiers for the 837 file to be populated. | No exceptions noted. |
| All claims submitted by the boards for overnight processing must contain a valid provider UPI (universal provider id – state), valid provider NPI (national provider id – federal) and provider tax id. | Entered claim submission scenarios in the test region to confirm edits were in place to require valid provider UPI, a valid provider NPI and completed provider tax ids. | No exceptions noted. |
| All claims submitted by the boards for processing are validated by a UNIX script on the file name and must contain a valid provider UPI with the correct ANSI (American National Standards Institute) version. | Inspected the email evidence sent by the ftp server on files rejected due to the wrong UPI number or the wrong version of the ANSI837P file being sent. | No exceptions noted. |

| **MACSIS -** *Control Objective:*<br>**Completeness of Input:** All authorized transactions are input and accepted for processing by MACSIS.<br><br>**Transaction Occurrence:** What assures that the claims recorded occurred and not fictitious? What prevents duplicate claims? | | ***Control Objectives Have 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. The status of processed claims (allowed, denied, etc.) is detailed in the Post-EDI Transaction Set Job Log and the .ASC Reports. | Entered a batch of claims into the test region from the period 1/1/14 to 12/31/14. Inspected the Diamond Claims EDI Detail Claims Reports that detailed the claims entered. Also inspected the Post-EDI Transaction Set Job Logs for the claims written to production and the .ASC Reports for the claim status.<br><br>Reentered the same claims as in the previous runs but with different file names into the test region. Inspected a second set of Diamond Claims EDI Detail Claims Reports, Post EDI Transaction Set Job Logs and .ASC Reports for a claim status of "duplicate" and “denied.” | No exceptions noted. |

| **MACSIS -** *Control Objective:*<br>**Accuracy of Input:** Authorized transactions are accurately recorded and in the proper period.<br><br>**Cutoff of Transactions**: What assures that claims are recorded in the proper period?<br><br>**Transaction Classification**: What assures that claims relate to and are coded to the proper account classification? | | ***Control Objectives Have Been Met*** |
|---|---|---|
| *Control Procedures:* | *Test Descriptions:* | *Test Results:* |
| Edits exist within Diamond 725 to increase the likelihood authorized transactions are accurately recorded. Edit errors are recorded on either the Diamond Claims EDI Critical Errors Report or the Diamond Claims EDI Non-Critical Errors Report. | Inspected the PREDI Error Code Listing and the following reports from March 2014 and November 2014 for evidence of edits in place:<br><br>1. Diamond Claims EDI Critical Errors Report.<br>2. Diamond Claims EDI Non-Critical Errors Report.<br><br>Also inspected a summary of critical errors and non-critical errors for March 2014 and November 2014. | No exceptions noted. |
| MACSIS will accurately process claim information based on pre-authorized input criteria. Non-Medicaid allowable rates are contained on the MACSIS fee schedule. | Obtained listings of MHAS contracts. Selected 60 contracts from the listing. Obtained the MACSIS fee schedule and an adjudicated claim listing relating to each MACSIS UPI contained on the sampled pre-authorized contracts.<br><br>Recalculated the amount allowed and amount paid on each contract and procedure code charged.<br><br>Confirmed the correct contracted amount was charged and paid. | No exceptions noted. |

| **MACSIS -** *Control Objective:*<br>**Completeness and Accuracy of Updating:** Updates, modifications, and/or additions to information already on MACSIS's database tables are accurately entered.<br><br>**Transaction Occurrence:** What assures that the claims recorded occurred and are not fictitious? What prevents duplicate claims?<br><br>**Existence:** What assures that the account balances exist as of the financial statement date? | | | ***Control Objectives Have Been Met*** |
|---|---|---|---|
| *Control Procedures:* | *Test Descriptions:* | *Test Results:* | |
| Changes to client Medicaid eligibility are electronically monitored by MACSIS for completeness and accuracy. | Inspected the MHHIPAA Diamond System Transaction Log Summary Control reports for 3/4/15, 3/5/15, and 3/6/15 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.<br><br>Also confirmed 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. | No exceptions noted. | |

| **MACSIS -** *Control Objective:*<br>**Integrity of Standing Data:** Changes to standing data are authorized and accurately input. | | ***Control Objective Has Been Met*** |
|---|---|---|
| *Control Procedures:* | *Test Descriptions:* | *Test Results:* |
| Non-Medicaid service rates, procedure code, and pricing information are maintained at the state level and entered by authorized personnel.<br><br>Procedure codes are updated by authorized personnel only. These rates and information are contained on various data files such as the Pricing Schedule (PROCP), Provider Contract Detail (PROVD), Provider Contract (PROVC), and Procedure Code (PROCD). Changes to these files are maintained in Diamond. | Obtained spreadsheets of all PROCP, PROVD, PROVC and PROCD changes as well as a listing of users with the logical access rights to update these files.<br><br>Used Excel to extract all changes that were made during CY 2014 for each file, and created a report listing by file of all user IDs that made these changes.<br><br>Compared the user listing with the Excel reports and inspected update capabilities to confirm only appropriate personnel had update capability. | No exceptions noted. |

| **MACSIS -** *Control Objective:*<br>**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 (non-recurring, claim specific info) 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.<br><br>Confirmed with appropriate MHAS personnel that all personnel with access to claims before adjudication were appropriate. | No exceptions noted. |

| **MACSIS -** *Control Objective:*<br>**Completeness and Accuracy of Accumulated Data:** The integrity of accumulated data is preserved. | | ***Control Objective Has Been Met*** |
|---|---|---|
| *Control Procedures:* | *Test Descriptions:* | *Test Results:* |
| 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 adjudicated and finalized.<br><br>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. | No exceptions noted. |

# SECTION 5 - OTHER INFORMATION PROVIDED BY THE SERVICE ORGANIZATION

| MACSIS USER BOARDS/CONSORTIA | | |
|---|---|---|
| **Board Name** | **Counties** | **Consortium** |
| Allen-Auglaize-Hardin | Allen, Auglaize, Hardin | N/A |
| Ashland | Ashland | Heartland East |
| Ashtabula | Ashtabula | Heartland East |
| Athens-Hocking-Vinton | Athens, Hocking, Vinton | N/A |
| Belmont-Harrison-Monroe | Belmont, Harrison, Monroe | Appcare |
| Brown | Brown | BHG (Behavioral Health Group) |
| Butler MH and ADAS | Butler | N/A |
| Champaign-Logan | Champaign, Logan | BHG(Behavioral Health Group) |
| Clermont | Clermont | N/A |
| Columbiana | Columbiana | Heartland East |
| Crawford-Marion | Crawford, Marion | PPS (Public and Private Solutions) |
| Cuyahoga ADAS | Cuyahoga | N/A |
| Cuyahoga MH | Cuyahoga | N/A |
| Delaware-Morrow | Delaware, Morrow | PPS (Public and Private Solutions) |
| Eastern Miami Valley | Clark, Greene, Madison | N/A |
| Erie-Ottawa | Erie, Ottawa | N/A |
| Fairfield | Fairfield | PPS (Public and Private Solutions) |
| Four County | Fulton, Henry, Defiance, Williams | N/A |
| Franklin | Franklin | N/A |
| Gallia-Jackson-Meigs | Gallia, Jackson, Meigs | N/A |
| Geauga | Geauga | N/A |
| Hamilton ADAS | Hamilton | N/A |
| Hamilton MH | Hamilton | N/A |
| Hancock | Hancock | BHG (Behavioral Health Group) |
| Huron | Huron | N/A |
| Jefferson | Jefferson | N/A |
| Lake | Lake | N/A |
| Licking-Knox | Licking, Knox | BHG (Behavioral Health Group) |
| Lorain ADAS | Lorain | N/A |
| Lorain MH | Lorain | N/A |
| Lucas ADAS | Lucas | N/A |
| Lucas MH | Lucas | N/A |
| Mahoning | Mahoning | Heartland East |
| Medina | Medina | Heartland West |

| MACSIS USER BOARDS/CONSORTIA | | |
|---|---|---|
| **Board Name** | **Counties** | **Consortium** |
| Miami-Darke-Shelby | Miami, Darke, Shelby | N/A |
| Montgomery | Montgomery | Montgomery |
| Muskingum | Muskingum, Coshocton, Guernsey, Morgan, Noble, Perry | N/A |
| Paint Valley | Pickaway, Fayette, Highland, Pike, Ross | Paint Valley |
| Portage | Portage | Heartland East |
| Preble | Preble | N/A |
| Putnam | Putnam | N/A |
| Richland | Richland | N/A |
| Ross | Ross | Paint Valley |
| Sandusky-Seneca-Union-Wyandot | Sandusky, Seneca, Union, Wyandot | BHG (Behavioral Health Group) |
| Scioto-Adams-Lawrence | Scioto, Adams, Lawrence | N/A |
| Stark | Stark | Heartland East |
| Summit | Summit | N/A |
| Trumbull | Trumbull | Western Reserve |
| Tusc-Carroll | Tuscarawas, Carroll | Heartland West |
| Van Wert-Mercer-Paulding | Van Wert, Mercer, Paulding | N/A |
| Warren-Clinton | Warren, Clinton | BHG (Behavioral Health Group) |
| Washington | Washington | N/A |
| Wayne-Holmes | Wayne, Holmes | Heartland East |
| Wood | Wood | N/A |

# Dave Yost • Auditor of State

**OHIO DEPARTMENT OF MENTAL HEALTH AND ADDICTION SERVICES**

**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**
**JULY 7, 2015**

88 East Broad Street, Fourth Floor, Columbus, Ohio 43215-3506
Phone: 614-466-4514 or 800-282-0370 Fax: 614-466-4490
**www.ohioauditor.gov**