

Audit Report

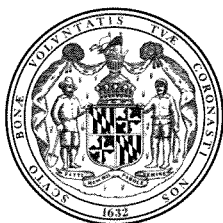
**Department of Health and Mental Hygiene
Mental Hygiene Administration**

September 2014



OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

-
- This report and any related follow-up correspondence are available to the public through the Office of Legislative Audits at 301 West Preston Street, Room 1202, Baltimore, Maryland 21201. The Office may be contacted by telephone at 410-946-5900, 301-970-5900, or 1-877-486-9964.
 - Electronic copies of our audit reports can be viewed or downloaded from our website at <http://www.ola.state.md.us>.
 - Alternate formats may be requested through the Maryland Relay Service at 1-800-735-2258.
 - The Department of Legislative Services – Office of the Executive Director, 90 State Circle, Annapolis, Maryland 21401 can also assist you in obtaining copies of our reports and related correspondence. The Department may be contacted by telephone at 410-946-5400 or 301-970-5400.
-



DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

September 18, 2014

Karl S. Aro
Executive Director

Thomas J. Barnickel III, CPA
Legislative Auditor

Senator James C. Rosapepe, Co-Chair, Joint Audit Committee
Delegate Guy J. Guzzone, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have conducted a fiscal compliance audit of the Mental Hygiene Administration (MHA) of the Department of Health and Mental Hygiene (DHMH) for the period beginning July 1, 2010 and ending October 7, 2013. MHA is responsible for developing comprehensive treatment and rehabilitation services for individuals with mental illness, and oversees the provision of publicly funded services that provide for the care and treatment of individuals who have mental disorders.

Our audit disclosed that MHA lacked adequate procedures for ensuring that documentation of patient eligibility was obtained and reviewed for services paid entirely with State general funds. These payments totaled approximately \$16.4 million during fiscal year 2013. In addition, certain contract deliverables were not received in a timely manner from a contractor used to monitor critical fiscal functions performed by MHA's Administrative Service Organization (ASO). The ASO provides benefit management services to MHA including authorizing services to consumers and paying providers. Our audit also disclosed that the ASO had not implemented certain security measures to enhance protection of MHA data, including sensitive consumer information.

DHMH's response to this audit, on behalf of MHA, is included as an appendix to this report. We wish to acknowledge the cooperation extended to us during the course of this audit by MHA.

Respectfully submitted,

Thomas J. Barnickel III, CPA
Legislative Auditor

Table of Contents

Background Information	4
Agency Responsibilities	4
Organizational Change	4
Status of Findings From Preceding Audit Report	4
Findings and Recommendations	5
Administrative Service Organization (ASO)	
* Finding 1 – MHA Lacked Adequate Procedures to Ensure That Documentation of Eligibility Was Obtained and Reviewed for Uninsured Patients	5
Finding 2 – Certain Contract Deliverables Were Not Received From an Independent Firm Hired to Monitor Critical ASO Activities	6
Information Systems Security and Control	
Finding 3 – The ASO’s Internal Network, Which Hosted MHA Information, Was Not Adequately Secured	8
Finding 4 – The ASO Stored Sensitive Information, Relating to MHA Consumers, and Did Not Adequately Restrict Access to the Sensitive Information	9
Cash Receipts	
* Finding 5 – Internal Controls Were Not Sufficient to Ensure All Receipts Were Deposited	10
Audit Scope, Objectives, and Methodology	12
Agency Response	Appendix

* Denotes item repeated in full or part from preceding audit report

Background Information

Agency Responsibilities

The mission of the Mental Hygiene Administration (MHA) is to promote the creation and management of a coordinated, comprehensive, accessible, culturally and age-appropriate system of publicly funded services and to support individuals who have mental disorders. To accomplish this mission, MHA develops comprehensive treatment and rehabilitation services for individuals with mental illness. In addition, MHA oversees the provision of publicly funded services that provide for the care and treatment of individuals who have mental disorders. Finally, MHA supervises State mental health facilities and reviews and approves local government plans for the treatment of the mentally ill through the monitoring of Core Service Agencies.¹ According to the State's records, MHA's expenditures totaled approximately \$788 million during fiscal year 2013 (mainly funded by State and federal funds) and were primarily for mental health services.

Organizational Change

Chapter 460, Laws of Maryland, 2014, effective July 1, 2014, merged the Mental Hygiene Administration and the Alcohol and Drug Abuse Administration to establish the Behavioral Health Administration within the Department of Health and Mental Hygiene (DHMH). According to the Fiscal and Policy Note accompanying the related legislation, this change was prompted, in part, by DHMH's examination of the issue of integrating substance use disorders and mental health care to address fragmentation in the delivery and government financing of those services. This organizational change had no impact on our audit since it occurred after the end of our audit period (October 7, 2013).

Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the eight findings contained in our preceding audit report on MHA dated July 12, 2011. We determined that MHA satisfactorily addressed six of these findings. The remaining two findings are repeated in this report.

¹ Core Service Agencies are county or multi-county authorities, such as a local health department or private provider, designated to receive funding from MHA to provide various mental health services to local jurisdictions throughout the State.

Findings and Recommendations

Administrative Service Organization

Background

The Mental Hygiene Administration (MHA) contracts with an Administrative Service Organization (ASO) to provide benefit management services, such as ensuring consumer eligibility, authorizing consumer services, and paying provider claims for the public mental health system. The ASO pays providers based on an established fee schedule and payments are made from a special bank account approved by the Comptroller of Maryland's General Accounting Division for this purpose. As claims are paid from the account, MHA processes reimbursements to the account.

During fiscal years 2011 through 2013, the ASO paid provider claims totaling approximately \$2 billion for mental health services, the vast majority of which related to consumers with Medicaid coverage, who are automatically eligible for mental health services through MHA. Medicaid covered services were eligible for federal fund participation (reimbursement) which is normally 50 percent of the claim payment. For its services during September 1, 2010 through August 31, 2013, the ASO contract fees totaled approximately \$31 million. MHA's current contract with the ASO will expire in February 2015.

Finding 1

MHA lacked adequate procedures to ensure that required documentation was obtained and verified to support patient eligibility for mental health services paid entirely by the State's General Fund.

Analysis

MHA lacked adequate procedures to ensure that required documentation was obtained by the providers and verified by MHA or the ASO to support patient eligibility for mental health services paid entirely by the State's General Fund (uninsured coverage). Individuals who do not qualify for Medicaid may still be eligible for mental health services paid by the State's General Fund if they meet certain eligibility criteria and qualifying conditions.

Although MHA provided guidance to providers regarding documentation requirements for uninsured coverage, our review of patients whose claims were paid exclusively with general funds disclosed that certain required eligibility documentation was not always on file. In this regard, we reviewed the eligibility documentation for 25 patients who had claims paid during the period from January through June 2013 totaling approximately \$235,000 under the uninsured coverage classification. These patients must meet six eligibility criteria and one

of several qualifying conditions. We determined that required documentation of a verifiable social security number and State residency (2 of 6 required eligibility criteria) was not available in 14 and 13 cases, respectively. Furthermore, we noted two cases in which the providers indicated the existence of the qualifying condition that the individuals had received services from the public mental health system within the last two years; however, documentation was not available to support this assertion.

In addition, the ASO, under its contract with MHA, is required to periodically examine selected providers and related claims for propriety, including a review of supporting eligibility documentation. However, the ASO's reviews of selected providers and related claims for propriety did not specifically target claims paid as uninsured coverage. Rather, the claims reviewed were chosen randomly and no statistics were kept on the number of claims paid as uninsured coverage that were audited.

During fiscal year 2013, the ASO paid claims totaling approximately \$16.4 million entirely with State general funds for patients granted uninsured coverage. The lack of adequate procedures for obtaining and verifying documentation of eligibility for uninsured coverage was commented upon in our two preceding audit reports.

Recommendation 1

We recommend that MHA establish procedures to ensure that required documentation supporting eligibility for individuals whose services are funded entirely with general funds is obtained in all cases, and verified, at least on a test basis (repeat).

Finding 2

MHA had not received all required contract deliverables from a firm which precluded effective monitoring of certain critical ASO fiscal activities.

Analysis

MHA was not receiving required contract deliverables, in a timely manner, from the independent public accounting firm it hired to perform reviews of certain critical ASO financial activities. Specifically, on May 25, 2011, MHA entered into a contract with a not to exceed value of \$369,220 for the period from May 2011 through August 2014 with the firm to review provider claims processed by the ASO and the ASO's monthly bank reconciliations of the State bank account used to pay those claims. The reviews of the claims and reconciliation were to be conducted by the firm on a quarterly basis, and draft reports on the results were to

be submitted to MHA 30 days after the end of the quarter. However, as of February 2014, the most recent report received by MHA for a claims review was for the quarter ending June 30, 2012. This report and the two preceding reports were received by MHA 19 to 21 months late. Similarly, the most recent report received for the firm's review of bank reconciliations was for the quarter ending December 31, 2012; this report and the four preceding reports were received 12 to 21 months late.

MHA contracted with the firm to perform certain agreed-upon procedures relating to provider claims and the ASO's bank account reconciliations, including ensuring proper claims authorization and record keeping, examining the submission of claims for federal reimbursement, and verifying the accuracy and validity of bank reconciliations and related reconciling items. These independent reviews are one of MHA's primary means to monitor critical functions performed by the ASO. Consequently, it is vital that MHA ensure that they are performed and the related reports are received timely. As of March 2014, payments to the contractor totaled approximately \$109,000 representing payments for billed services rendered from inception of the contract through November 2012.

Recommendation 2

We recommend that MHA ensure that all contract deliverables, such as the aforementioned claims and bank reconciliation reviews and resulting reports, are performed and received within the required time frames.

Information Systems Security and Control

Background

As noted, MHA contracts with an ASO to provide mental health benefit management services. The ASO's system processed various information related to the provision of mental health services and captured and stored typical demographic information for MHA consumers, including name, social security number, address, and date of birth. The system also captured and stored sensitive personal health information, including but not limited to, medical diagnosis codes, prescribed medications, and physician assessments of patient risks, impairments, and substance abuse. The system was hosted at the ASO's national data center facility located in a neighboring state.

Finding 3

The ASO's internal network, which hosted MHA information, was not adequately secured.

Analysis

The ASO's internal network, which hosted MHA information, was not adequately secured.

- Several unnecessary and insecure connections were allowed to portions of the ASO's internal network, thereby placing various network devices at risk. For example, we noted that three third party networks (owned by two current ASO clients and one terminated ASO client) had unnecessary access to almost all destinations on the ASO internal network via all ports. Best practice guidelines from the State of Maryland Department of Information Technology *Information Security Policy* require that State agency systems be configured to monitor and control communications at external boundaries.
- We identified 61 ASO internal network addresses which could receive encrypted traffic and did not have Host-based Intrusion Protection System (HIPS) coverage. The absence of HIPS coverage for traffic to these network addresses created a security risk since the ASO's network based intrusion detection prevention system cannot read encrypted traffic flowing into or out of its network, whereas HIPS can read and analyze such traffic and protect critical servers from malicious traffic. Strong network security uses a layered approach, relying on various resources structured according to assessed network security risks. Complete Intrusion Detection/Protection System (IDPS) coverage includes, when there is encrypted traffic, the use of a network-based IDPS that is supplemented with HIPS to aid significantly in the detection/prevention of, and response to, potential network security breaches and attacks.

Recommendation 3

We recommend that MHA ensures that the ASO

- a. restricts access, at the network level, to key administrative resources to only those entities requiring such access; and**
- b. performs a documented review and assessment of its network security risks, identifies how HIPS coverage should be best applied to its network, and implements such coverage.**

Finding 4

The ASO stored sensitive personally identifiable information, relating to MHA consumers, in clear text and did not adequately restrict access to sensitive information.

Analysis

The ASO stored sensitive personally identifiable information (PII), relating to MHA consumers, in clear text and did not adequately restrict access to sensitive information.

- The ASO stored MHA consumer PII (including full names, social security numbers, and dates of birth for approximately 152,000 MHA consumers) in clear text within a master file and 45 separate database tables. We further noted that the sensitive information stored in the database tables was not masked or truncated when system users accessed this data. This sensitive PII, which is commonly sought by criminals for use in identity theft, should be protected by appropriate information system security controls. Best practice guidelines from the State of Maryland Department of Information Technology (DoIT) *Information Security Policy* require each State agency to “protect confidential data using encryption technologies and/or other substantial mitigating controls.”
- Users were granted unnecessary read and modification access to certain critical ASO files containing sensitive PII for Maryland Medicaid enrollees (including MHA consumers). For example, 15 profiles had unnecessary read access to a critical table containing full names, social security numbers, and dates of birth of numerous Maryland Medicaid enrollees. The DoIT *Information Security Policy* requires “only authorized individuals (employees or agency contractors) have access to confidential information and that such access is strictly controlled, audited, and that it supports the concepts of ‘least privilege’ and ‘need to know.’”

Recommendation 4

We recommend that MHA request that the ASO

- a. encrypt all files and database objects containing MHA consumer PII,**
- b. mask or truncate social security numbers applicable to MHA consumers from online database and application users that do not need to see the full number, and**
- c. restrict read and modification access to critical and sensitive Maryland Medicaid enrollees’ information to only those personnel who require such access.**

Cash Receipts

Finding 5

Internal controls over cash receipts were not sufficient to ensure all receipts were deposited.

Analysis

MHA had not established adequate procedures and internal controls over its cash receipts to provide assurance that all collections were deposited intact.

- MHA did not verify that collections received through the mail, which totaled approximately \$741,000 during fiscal year 2013, were forwarded to and received by the Department of Health and Mental Hygiene (DHMH) general accounting unit for deposit. These receipts, which related primarily to refunds or cost settlements due from providers, were initially recorded on a check log by MHA then forwarded to the unit for processing. Although the unit provided a receipt to MHA for the funds, the receipt was not agreed to the check log by independent personnel to ensure that all recorded collections were transferred to and received by the unit. Furthermore, the employee who first received the mail collections was responsible for maintaining the related record of amounts due from providers.
- Collections received at MHA's Crownsville Hospital Center were not adequately controlled and verified to deposit.² These collections, which totaled approximately \$251,000 during fiscal year 2013, were first received and recorded at the Center and then forwarded to MHA headquarters for processing and deposit. However, an independent verification of collections received at the Center to validated bank deposit documentation was not performed. Furthermore, the employee who received the Center's collections at MHA headquarters was also responsible for mailing related monthly invoices to tenants and for recording the related payments in the accounts receivable records.

Similar conditions regarding the verification of recorded collections to deposit were commented upon in our two preceding audit reports.

² Although the Crownsville Hospital Center is closed, certain areas of the facility are leased to various entities. Collections received at the Center represent payments from those tenants for their share of utility costs.

Recommendation 5

We recommend that MHA

- a. designate an employee independent of the cash collection functions to verify recorded collections to the receipt from DHMH or validated bank documentation, as appropriate (repeat); and**
- b. ensure that employees who receive collections do not also maintain the related accounts receivable records.**

We advised MHA on accomplishing the necessary separation of duties using existing personnel.

Audit Scope, Objectives, and Methodology

We have conducted a fiscal compliance audit of the Mental Hygiene Administration (MHA) of the Department of Health and Mental Hygiene (DHMH) for the period beginning July 1, 2010 and ending October 7, 2013. The audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

As prescribed by the State Government Article, Section 2-1221 of the Annotated Code of Maryland, the objectives of this audit were to examine MHA's financial transactions, records, and internal control, and to evaluate its compliance with applicable State laws, rules, and regulations.

In planning and conducting our audit, we focused on the major financial-related areas of operations based on assessments of significance and risk. The areas addressed by the audit included claims payments for treatment and rehabilitation services as managed by an Administrative Service Organization (ASO), monitoring of Core Service Agencies, cash receipts, and information system security and control. We also determined the status of the findings contained in our preceding audit report.

To accomplish our audit objectives, our audit procedures included inquiries of appropriate personnel, inspections of documents and records, observations of MHA's operations, tests of transactions, and a site visit to the ASO's national data center. We also performed various data extracts of pertinent information from the State's Financial Management Information System (such as revenue and expenditure data). The extracts are performed as part of ongoing internal processes established by the Office of Legislative Audits and were subject to various tests to determine data reliability. We determined that the data extracted from these various sources were sufficiently reliable for the purposes the data were used during this audit. In addition, we obtained data extracted from the ASO's automated records for the purpose of testing selected attributes relating to providers and provider claims paid. We performed various tests of the relevant data and determined that the data were sufficiently reliable for the purposes the data were used during the audit. Finally, we performed other auditing procedures that we considered necessary to achieve our objectives. The reliability of data used in this report for background or informational purposes was not assessed.

Our audit did not include certain support services provided to MHA by DHMH's Office of the Secretary. These support services (such as payroll processing, purchasing, maintenance of accounting records, and related fiscal functions) are included within the scope of our audit of DHMH - Office of the Secretary. In addition, our audit did not include an evaluation of internal controls for federal financial assistance programs and an assessment of MHA's compliance with federal laws and regulations pertaining to those programs because the State of Maryland engages an independent accounting firm to annually audit such programs administered by State agencies, including MHA.

MHA's management is responsible for establishing and maintaining effective internal control. Internal control is a process designed to provide reasonable assurance that objectives pertaining to the reliability of financial records, effectiveness and efficiency of operations including safeguarding of assets, and compliance with applicable laws, rules, and regulations are achieved.

Because of inherent limitations in internal control, errors or fraud may nevertheless occur and not be detected. Also, projections of any evaluation of internal control to future periods are subject to the risk that conditions may change or compliance with policies and procedures may deteriorate.

Our reports are designed to assist the Maryland General Assembly in exercising its legislative oversight function and to provide constructive recommendations for improving State operations. As a result, our reports generally do not address activities we reviewed that are functioning properly.

This report includes findings related to conditions that we consider to be significant deficiencies in the design or operation of internal control that could adversely affect MHA's ability to maintain reliable financial records, operate effectively and efficiently, and/or comply with applicable laws, rules, and regulations. Our report also includes findings regarding significant instances of noncompliance with applicable laws, rules, or regulations. Other less significant findings were communicated to MHA that did not warrant inclusion in this report.

The response from DHMH, on behalf of MHA, to our findings and recommendations is included as an appendix to this report. As prescribed in the State Government Article, Section 2-1224 of the Annotated Code of Maryland, we will advise DHMH regarding the results of our review of its response.

APPENDIX



STATE OF MARYLAND

DHMH

Maryland Department of Health and Mental Hygiene

201 W. Preston Street • Baltimore, Maryland 21201

Martin O'Malley, Governor – Anthony G. Brown, Lt. Governor – Joshua M. Sharfstein, M.D., Secretary

September 17, 2014

Mr. Thomas J. Barnickel III, CPA
Legislative Auditor
Office of Legislative Audits
301 West Preston Street
Baltimore, MD 21201

Dear Mr. Barnickel:

Thank you for your letter regarding the draft audit report for the Department of Health and Mental Hygiene – Mental Hygiene Administration for the period beginning July 1, 2010 through October 7, 2013. Enclosed you will find the Department's response and plan of correction that addresses each audit recommendation.

I will work with the appropriate Administration Directors, Programs Directors, and the Deputy Secretary to promptly address the audit exceptions. In addition, the OIG's Division of Internal Audits will follow-up on the recommendations to ensure compliance.

If you have any questions or require additional information, please do not hesitate to contact Thomas V. Russell, Inspector General, at 410-767-5862.

Sincerely,

Joshua M. Sharfstein, M.D.
Secretary

cc: Gayle Jordan-Randolph, M.D., Deputy Secretary, Behavioral Health and Disabilities, DHMH
Brian Hepburn, M.D., Executive Director, Behavioral Health Administration, DHMH
Daryl Plevy, J.D., Deputy Director, Behavioral Health Administration, DHMH
Thomas V. Russell, Inspector General, DHMH
Ellwood L. Hall, Assistant Inspector General, DHMH
Rianna Matthews-Brown, Acting Chief of Staff, DHMH

Toll Free 1-877-4MD-DHMH – TTY/Maryland Relay Service 1-800-735-2258

Web Site: www.dhmh.maryland.gov

Administration's Response to Findings and Recommendations

Finding 1

MHA lacked adequate procedures to ensure that required documentation was obtained and verified to support patient eligibility for mental health services paid entirely by the State' General Fund.

Recommendation 1

We recommend that MHA establish procedures to ensure that required documentation supporting eligibility for individuals whose services are funded entirely with general funds is obtained in all cases, and verified, at least on a test basis (repeat).

Administration's Response:

MHA concurs with the recommendation and has established procedures to ensure documentation supporting eligibility for individuals whose services are paid for entirely with general funds. With implementation of the Affordable Care Act, the number of uninsured individuals and uninsured services is decreasing. Since the last audit, MHA has improved the requirements for documentation which have been disseminated through four Provider Alerts. During the process of implementing these new requirements, it was determined there are times when providers cannot obtain the expected documentation when consumers are in crisis, either because the individual is too ill to provide needed information or because the service provided is time limited in nature. If MHA's policies become too restrictive for people who are unstable or in crisis, this may cause undue risk to consumers and public safety. When providers see a consumer on a regular basis, they are able to obtain the needed documentation once the individual is stabilized, but when a person is seen on a time limited basis, the cost of obtaining the documentation is greater than the savings of requiring it in a crisis and/or the risks associated with overly restrictive barriers to service access.

Exceptions to the documentation requirement are related to the type of crisis and type of service. If a consumer is in immediate need for services (such as acutely suicidal) or the consumer's symptoms prevent that person with being able to provide information and they are being seen by an Assertive Community Treatment team, mobile crisis, residential crisis program, or other outpatient setting documentation criteria may be waived. If the consumer is seen by the program for more than two visits/days, all documentation must be submitted per requirements. Documentation will be verified on a test basis. A Provider Alert clarifying the exceptions will be disseminated in October 2014.

Additionally, the Administrative Services Organization (ASO) will undertake a number of measures to ensure that documentation are received in a timely manner from those providers who are rendering services for longer periods of time.

The ASO will assist MHA with education for providers and review of their documentation in addition to the current auditing process using the following mechanisms:

- The ASO will host provider meetings to identify the root cause(s) of providers failing to secure the evidence of uninsured eligibility and will follow-up with a work group to address these obstacles. A list of recommendations will be generated for MHA review.
- Through data reporting, the ASO will identify providers with the highest volumes of uninsured consumers. ASO staff will do on-site visits with these providers to review their process for assuring adequate documentation and train them on best practices for securing evidence of uninsured eligibility. The ASO will work with MHA to define the threshold to target appropriate providers.
- The ASO will host webinars and disseminate Provider Alerts twice a year to review best practices for obtaining and retaining all required documentation for uninsured eligibility.
- Providers of initial uninsured eligible visits who have not yet secured all necessary documentation will be asked to provide a case management referral for the initial period of the uninsured authorization, to help make sure that someone is available to help the consumer with obtaining the needed documentation and entitlements.

Finding 2

MHA had not received all required contract deliverables from a firm which precluded effective monitoring of certain critical ASO fiscal activities.

Recommendation 2

We recommend that MHA ensure that all contract deliverables, such as the aforementioned claims and bank reconciliation reviews and resulting reports, are performed and received within the required time frames.

Administration's Response:

MHA concurs with the recommendation. When the contract was signed with the independent accounting firm there was a backlog of audits that needed to be performed.

MHA has been working with the partner at the independent accounting firm in order to get the reviews up to date, and has been holding payments pending promised deliverables. Currently, the most recent draft bank reconciliation report reviewed by MHA was the September 2013 report. The Administration anticipates that the contractor will be up to date with deliverables by December 31, 2014. The contract with the vendor has been extended until June 30, 2015. The partner has developed a new schedule for the deliverables to bring the reporting up to date and to meet deliverables on time in the future.

Finding 3

The ASO's internal network, which hosted MHA information, was not adequately secured.

Recommendation 3

We recommend that MHA ensures that the ASO

- a. restricts access, at the network level, to key administrative resources to only those entities requiring such access; and**
- b. performs a documented review and assessment of its network security risks, identifies how HIPS coverage should be best applied to its network, and implements such coverage.**

Administration's Response:

- a. MHA concurs with the recommendation for restricting access, at the network level, for key administrative resources to only those entities requiring such access. The ASO resolved these items as they were being identified by the State auditors during the course of the fieldwork. All access is tightly controlled and monitored. The ASO shall continue to follow a "least privilege" security strategy to protect confidentiality, integrity, and availability of the information with which it is entrusted.
- b. MHA concurs with the recommendation to perform a documented review and assessment of its network security risks to identify how HIPS coverage can be applied to its network. The ASO has completed its review/assessment and based on the review/assessment findings, the ASO is expanding its current HIPS implementation to all of its public facing resources to monitor control communications at external boundaries. In addition, the ASO is adding an additional safeguard for Layer 7 protection through the implementation of a network based web application firewall to monitor both encrypted and unencrypted traffic. The ASO is waiting on final testing to be placed in production. The estimated completion date is by the end of 2014.

Finding 4

The ASO stored sensitive personally identifiable information, relating to MHA consumers, in clear text and did not adequately restrict access to sensitive information.

Recommendation 4

We recommend that MHA request that the ASO

- a. encrypt all files and database objects containing MHA consumer PII,**
- b. mask or truncate social security numbers applicable to MHA consumers from online database and application users that do not need to see the full number, and**
- c. restrict read and modification access to critical and sensitive Maryland Medicaid enrollees' information to only those personnel who require such access.**

Administration's Response:

- a. MHA concurs with the recommendation to encrypt all files and database objects containing MHA consumer PII. The ASO is in the process of evaluating solutions to protect PII database objects through at rest encryption. The ASO estimates that this will be completed by March 2015.
- b. MHA concurs with the recommendation to mask or truncate social security numbers applicable to MHA consumers from online database and application for users that do not need to see the full number. The ASO is in the process of evaluating software changes that will truncate/mask social security numbers during viewing. The ASO estimates that this will be completed by March 2015. Please note the data is protected at multiple levels and is only accessible by a select group of users who are able to generate and review the output. This data is not, and has never been, publicly available.
- c. MHA concurs with the recommendation to restrict read and modification access to critical and sensitive Maryland Medicaid enrollees' information to only those personnel who require such access. The ASO resolved these items as they were being identified by the State Auditors during the course of the fieldwork. In addition, ASO has further strengthened its "Discretionary Role Based Access Control" to restrict access to critical and sensitive Maryland Medicaid enrollee data by limiting access to select authorized individuals only.

Finding 5

Internal controls over cash receipts were not sufficient to ensure all receipts were deposited.

Recommendation 5

We recommend that MHA

- a. **designate an employee independent of the cash collection functions to verify recorded collections to the receipt from DHMH or validated bank documentation, as appropriate (repeat); and**
- b. **ensure that employees who receive collections do not also maintain the related accounts receivable records.**

We advised MHA on accomplishing the necessary separation of duties using existing personnel.

Administration's Response:

- a. MHA concurs with the recommendation and will establish a revised segregation of duties plan using existing personnel. MHA will utilize an existing employee in a manner to better show segregation of duties and apply the procedures to mail receipts and making Crownsville receipts mail receipts as well.

Effective immediately, mail receipts will be opened by the Administrative Assistant for the Director of Services and record checks in a log upon receipt. MHA will ensure that an employee independent of the cash collection functions verifies the initial record of collections received to either the receipt from DHMH or validated bank documentation as appropriate. Effective immediately MHA's Accountant Advanced will verify the initial record collections received to the receipt from DHMH.

MHA will ensure that employees who receive collections do not also maintain the related accounts receivable records. Mail for the Director of Fiscal Services will be opened by the Administrative Assistant and checks, if any, will be recorded by her. The Accountant Technician will be responsible for depositing the check, and preparation of the deposit memo to DHMH. The Director of Fiscal Services will initial the deposit memo to DHMH to review PCA coding to FMIS. The written policies and procedures will be updated to incorporate the new procedures.

In regard to Crownsville receipts, all checks will be received, opened, and logged by the Administrative Assistant. The Accountant Supervisor will verify the initial record of collections with the validated bank documentation.

- b. MHA concurs with the recommendation and all incoming checks will be received by the Administrative Assistant, deposited by the Accountant Advanced, and the Account Technician will verify the payment with the invoice. The written policies and procedures will be undated to incorporate the new procedures.

AUDIT TEAM

Paul R. Denz, CPA

Audit Manager

Richard L. Carter, CISA

Steven P. Jersey, CPA, CISA

Information Systems Audit Managers

Michael J. Murdzak, CPA

Senior Auditor

Michael K. Bliss, CISA

John C. Venturella

Information Systems Senior Auditors

Marissa L. Eby

Sam Hur

Lauren E. McLain

Olajide S. Mustapha

Staff Auditors

Matthew D. Walbert

Information Systems Staff Auditor