Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump
Making government work better

Official Audit Report – Issued August 13, 2012

Review of the Internal Controls Established by the Executive Office of Health and Human Services and MassHealth over Selected Information System Applications

For the period January 1, 2010 through June 30, 2011

State House Room 230 ■ Boston, MA 02133 ■ auditor@sao.state.ma.us ■ www.mass.gov/auditor

TABLE OF CONTENTS/EXECUTIVE SUMMARY

The Massachusetts Executive Office of Health and Human Services (EOHHS) is one of the largest Secretariats within the Commonwealth, with an annual budget that equals approximately 52% of the Commonwealth's total operating expenditures. The Massachusetts Medicaid program, known as MassHealth, which provides access to healthcare services to approximately 1.3 million eligible low- and moderate-income individuals, couples, and families annually, falls within EOHHS. In fiscal year 2011, MassHealth paid in excess of $12.2 billion to health care providers, of which approximately 40%[1] was funded with Commonwealth funds.

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an audit of the information technology (IT) controls associated with two of MassHealth's mission-critical applications[2]: its Medicaid Management Information System (MMIS) that it uses to process claims from its service providers and its MA21 eligibility determination system that it uses to determine both applicants' and members' eligibility for benefits and their level of benefits. Our audit, which covered the period January 1, 2010 through June 30, 2011, included a review of the internal controls established by EOHHS and MassHealth in the areas of access security over these applications, Criminal Offender Record Information (CORI) background checks on employees working with these applications, and the protection of personal identifiable information residing within these applications. In addition, we evaluated EOHHS's and MassHealth's contingency planning in accordance with Executive Order No. 490, including a review of their continuity of operations planning, business continuity planning, and disaster recovery planning, including on-site and off-site storage of backup magnetic media.

Based on our audit, we determined that during the audit period, EOHHS and MassHealth maintained adequate internal controls in the reviewed areas relative to CORI checks, the protection of personal information, and disaster recovery planning. However, as discussed in the Audit Results section of this report, we found that improvements were needed in EOHHS's logical access security controls and both EOHHS's and MassHealth's contingency planning.

Our audit disclosed that EOHHS had established adequate password administration and security procedures over MassHealth's network resources, including its MMIS and MA21 applications. However, some of these procedures, particularly those regarding the timely deactivation or deletion of network user accounts for staff and contractors who are no longer employed by MassHealth, were not being followed. As a result, we found that a significant number of user accounts remained active for individuals who were no longer authorized to have access to MassHealth's network or the MA21 and MMIS applications,

[1] The Federal Medical Assistance Percentage (federal matching funds) for state Medicaid expenditures is 50%. However, as a result of the American Recovery and Reinvestment Act, the federal reimbursement rate during our audit period, including fiscal year 2011, was 65%.

[2] A mission-critical application is any process that is critical to the continued operation of the organization.

[3] Certain health information is considered "protected health information" under the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996.

INTRODUCTION

Background

The Massachusetts Executive Office of Health and Human Services (EOHHS) is one of the largest Secretariats within the Commonwealth, with an annual budget that equals approximately 52% of the Commonwealth's total operating expenditures. The Massachusetts Medicaid program, known as MassHealth, which provides access to healthcare services to approximately 1.3 million eligible low- and moderate-income individuals, couples, and families annually, falls within EOHHS. In fiscal year 2011, MassHealth paid in excess of $12.2 billion to health care providers, of which approximately 40% was funded with Commonwealth funds.

EOHHS is responsible for working with MassHealth in establishing the internal controls over MassHealth's computer applications and administering these controls once established. MassHealth's mission-critical applications include the Virtual Gateway, its Medicaid Management Information System (MMIS), and its MA21 eligibility system. The Virtual Gateway is an internet portal designed by EOHHS to provide the general public, medical providers, community-based organizations, and EOHHS staff with online access to information on health and human service programs. MMIS is MassHealth's automated claims processing system that it uses to pay its providers. The MA21 system is MassHealth's eligibility determination system used to capture MassHealth member data as it is received on MassHealth's benefit application forms; requests for updated information forms; and eligibility-related data from other sources such as pay stubs, birth records, and other documents supplied by applicants and members for the purposes of determining applicants' and members' eligibility for benefits and their level of benefits. The MA21 system is hosted on a mainframe platform at the Massachusetts Information Technology Center managed by EOHHS's Information Technology Organization (ITO).

Audit Scope, Objectives, and Methodology

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an audit of the information technology (IT) controls associated with two of MassHealth's mission-critical applications: its MA 21 eligibility and MMIS systems. Our audit, which covered the period January 1, 2010 through June 30, 2011, 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.

The scope of our audit included a review of the internal controls established by EOHHS and MassHealth in the following areas: access security over the applications reviewed, Criminal Offender Record Information (CORI) background checks on employees working with these applications, the protection of personal identifiable information within these applications, continuity of operations planning, business continuity planning, and disaster recovery planning, including on-site and off-site storage of backup magnetic media.

In order to achieve our audit objectives, we first reviewed all applicable laws, regulations, and other criteria applicable to our engagement. These included Chapter 93H of the General Laws; Executive Orders No. 490 and No. 504; Chapter 82 of the Acts of 2007; Chapter 647 of the Acts of 1989; management policies and procedures; and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT version 4.1) issued by the Information Systems Audit and Control Association in July 2007.

To achieve our audit objectives, we:

- Determined whether EOHHS's IT policies and procedures provided management and system users with sufficient standards and guidelines to describe, review, and comply with statutes, regulations, policy directives, and generally accepted control objectives for IT operations and security.

- Assessed the adequacy of the planning, design, development, and testing of program changes to the MA21 and MMIS applications during the period January 1, 2010 through June 30, 2011.

- Reviewed IT-related policies and procedures for the areas under review and determined whether written, authorized, and approved policies and procedures had been implemented, including policies and procedures for authorizing, activating, and deactivating system access privileges to the local area network and the MA21 and MMIS applications.

- Interviewed senior management and reviewed MassHealth's procedures and control practices to determine whether CORI checks were performed prior to employment or for a change in position responsibility.

- Interviewed senior management and reviewed MassHealth's completed Self-Audit Questionnaire and Information Security Program, which includes an Electronic Security Plan, to determine MassHealth's compliance with Chapter 93H of the General Laws and Executive Order 504 regarding protection of personally identifiable information and notification of confidentiality breaches.

- Determined whether a formal continuity of operations plan was in place that would work in conjunction with both the business continuity plan and disaster recovery plan strategies to restore mission-critical and essential operations and enable EOHHS and MassHealth to continue its daily operations in a timely manner should computing systems be unavailable for an extended period.

- Evaluated the level of risk associated with the program changes being made by EOHHS's Information Technology Organization in terms of their potential for improperly disclosing personal information that is accessed through the network residing on MassHealth's MA21 and MMIS applications.

We found that during our audit period, EOHHS had established adequate password administration and security procedures over MassHealth's network resources, including its MMIS and MA21 applications. We also determined that EOHHS's internal Information Technology Organization (ITO) had established password-administration and security procedures relative to authorizing and activating user privileges for access to MassHealth network resources. These controls established specific requirements for password creation, expiration, logon, and configuration. We also found that the ITO had a formal security access request process in place for providing and administering access rights to all EOHHS networks, network resources, applications, databases, data sets and other non-EOHHS-owned applications used by staff and contractors. Further, we determined that there were adequate procedures in place that require new hires and contractors of EOHHS to receive a Criminal Offender Record Information check and acknowledge compliance with EOHHS and the Commonwealth's Information Technology Department's security policies concerning acceptable use of network resources. Finally, we determined that in September 2010, the Social Security Administration conducted an onsite system security review and found no weaknesses in MassHealth's controls to verify and retain Social Security numbers consistent with the terms of their information exchange agreement.

However, as discussed in the Audit Results section of this report, we found that improvements were needed in EOHHS's user access security controls and both EOHHS's and MassHealth's contingency planning.

AUDIT RESULTS

1. IMPROVEMENTS NEEDED IN USER ACCESS SECURITY CONTROLS

The Executive Office of Health and Human Services (EOHHS) needs to strengthen EOHHS's and MassHealth's user access security controls in certain areas. First, the user access procedures established by EOHHS, particularly those regarding the timely deactivation or deletion of network user accounts for staff and contractors who are no longer employed by MassHealth or are transferred to other agencies within the Commonwealth were not being followed. Further, EOHHS's internal Information Technology Organization (ITO) did not conduct annual access reviews as required by ITO policies. As a result, we found that a significant number of user accounts remained active for individuals who were no longer authorized to have access to the MassHealth network or the MA21 and MMIS systems. Our tests revealed that of the 1,124 directory network user accounts that were active during our audit period, 112 (10%) of these accounts were associated with individuals who no longer worked at MassHealth. In addition, we found that 289 (27%) of the 1,059 MA21 user accounts and 488 (33%) of the 1,462 MMIS user accounts were associated with individuals who no longer worked at MassHealth. The failure to deactivate user accounts in a timely manner places MassHealth at risk of individuals obtaining unauthorized access to restricted information.

In addition, we found that the ITO did not have formal, enterprise-wide security policies and procedures for all EOHHS agencies that governed user access to network resources, including MassHealth's MA21 and MMIS applications, that would enable management to guide operations in a consistent manner and allow employees to understand their roles and responsibilities within predefined limits. However, during our audit, the ITO was in the process of formalizing such enterprise-wide policies and procedures for all IT-related security functions.

Finally, we determined that third-party contractors/software developers performing program changes to the mission-critical application systems we reviewed unnecessarily had access to the personal information contained in these applications, which contain protected health information, when testing their software changes. Although we did not view this as an internal control deficiency, since developers work within a secured test environment, access to such personal information should be limited.

Recommendation

We recommend that EOHHS's user access security controls be strengthened by:

- Ensuring that access privileges for unauthorized users are deactivated or modified when a change in an employee's status results in the user no longer requiring access to IT resources, or when a change in an employee's position or responsibilities requires a change in access privileges.

- Implementing formal notification procedures requiring that EOHHS/MassHealth human resources or department management notify ITO personnel of all changes in employee status, such as terminations, extended leaves of absence, or transfers. In addition, the ITO should periodically issue reports to identify those users who have not logged on for a period of 60 days or more as determined by ITO management. This will help to ensure that sufficient security controls are in place to protect the confidentiality and integrity of sensitive data and to limit access to data and system functions to only authorized parties.

- Enforcing ITO policies and initiating controls to conduct an annual review of all user IDs that have access to applications containing personally identifiable information or of additional applications as specified by management.

- Aggressively pursuing completion of the ITO's enterprise-wide policies and procedures for all IT security initiatives. Formally documented policies and procedures will enable IT management to ensure compliance with existing rules and regulations and help mitigate the risks associated with unauthorized use of user accounts.

- In accordance with the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996, using data-masking software during program changes to obscure sensitive personal information by replacing actual data with artificial data. The ITO should work with its third-party contractors and/or software developers to identify a practical and cost-effective data-masking application to prevent unauthorized access to personal information.

Auditee's Response

EOHHS will formalize and implement a new Security Request Process using CA Unicenter and will reissue the Security Request Policy which states that "When requesting access to or a change in access to MIS Resources a Security Request Form, must be completed, authorized by the Users Director or Assistant Director, and submitted to the IT Security Operations Unit. This form is required to be completed by the Director when an employee is hired, transferred, promoted, demoted, terminated or at any other time that an employees' access level or job function changes." . . .

In addition the EOHHS Personal Liaisons and EOHHS IT Personnel Department will notify EHS Security Operations of all user terminations. EOHHS agrees with your

recommendation and will produce biannual reports to identify and inactivate those users who have not logged into the Network for over 90 days.

EOHHS agrees with your findings [regarding controls over personally identifiable information] and are looking into the mechanics by which we can accomplish an annual review.

EOHHS will continue to participate in the Enterprise Security Boards Policy Committee to produce enterprise policies and standards and will continue to pursue the completion of EOHHS enterprise-wide security policies and procedures.

ITD [the Commonwealth's Information Technology Division] has existing data masking software that may be available for EOHHS purposes. An EOHHS IT manager is in the process of reviewing the ITD solution and will pursue the feasibility and affordability of adopting the software. A report will be issued to IT senior and executive staff before the close of SFY12.

2. IMPROVEMENTS NEEDED IN CONTINGENCY PLANNING

Our audit identified inadequacies in EOHHS's and MassHealth's contingency planning. Specifically, we found that (a) EOHHS did not have an updated Continuity of Operations Plan (COOP) that focuses on restoring and performing essential functions at an alternate site on an enterprise-wide basis and (b) MassHealth did not have a Business Continuity Plan (BCP) that focuses on sustaining its business functions during and after a disruption, as discussed below.

a. Continuity of Operations Plan

Contrary to state law, EOHHS has not been updating its COOP annually. In fact, EOHHS's COOP has not been updated since May 2009. Since 1978, state agencies, including those within EOHHS, have been required by executive order to perform and document their planning efforts for the continuity of operations and government. Specifically, Executive Order No. 490 issued in September 2007 states, in part:

> *Whereas, to achieve a maximum state of readiness, these plans should be incorporated into the daily operations of every secretariat and agency in the executive department, and should be reviewed on a regular basis and, with respect to agencies supplying services critical in times of emergency, exercised regularly. In addition, each critical secretariat and agency shall submit an annual report to the Executive Office of Public Safety and Security.*

According to EOHHS officials, this is because over the past few years, EOHHS underwent organizational restructuring and its senior management neglected to assign the responsibility of updating the agency's Continuity of Operations Plan to an appropriate staff person in the new organizational structure.

Recommendation

EOHHS should:

- Update its COOP to comply with the requirements of Executive Order No. 490 regarding the creation, documentation, maintenance, and training required to prepare for emergencies and disasters and provide the updated copy of the COOP to the Massachusetts Emergency Management Agency (MEMA) for coordinating resources, training, and operations.

- Ensure that the updated COOP documents procedures that work in concert with business continuity and disaster recovery plans that would allow for the uninterrupted delivery of EOHHS's and MassHealth's essential functions.

Auditee's Response

MassHealth's Chief Operating Officer worked with MassHealth Operations to update the COOP/COG plans and has a draft under review by the Executive Office of Health and Human Services and once finalized will be reviewed annually.

b. Business Continuity Plan

MassHealth did not have a formal, documented BCP that would help ensure that mission-critical business operations can be recovered in a timely manner. Specifically, MassHealth did not develop or document contingency plans for its primary business functions in the event of a potential loss of computing capabilities. As a result, MassHealth is vulnerable to a disruption of services that could have an impact on residents of the Commonwealth should IT capabilities be rendered inoperable for an extended period of time. Business continuity planning is an essential part of continuing MassHealth's business operations, and generally accepted business practices and industry standards for computer operations recommend the need for MassHealth to have an ongoing business continuity planning process that can document access to systems on which it depends for processing or operational needs.

The Commonwealth's Information Technology Division (ITD) within the Executive Office for Administration and Finance, in conjunction with a contracted vendor (SunGard Availability Services), provides disaster recovery services to MassHealth for its mission-critical systems, including off-site storage of electronic back-up copies. In this role, ITD serves as a service bureau to MassHealth, providing a critical part of the necessary requirements for business continuity planning. Without a BCP, MassHealth risks not being able to support its clients if

connections to ITD's network are lost. Since ITD maintains the systems that support MassHealth's applications, the business continuity planning process should include instructions on how to coordinate with ITD, should network connectivity be interrupted. Significant delays can occur when users, including health care providers and recipients of health care benefits, are not able to access the network in a reasonable timeframe, thereby causing backups in the input of critical health-related information.

Recommendation

MassHealth should:

- Work with ITD and EOHHS to develop a comprehensive BCP that would ensure that MassHealth is able to access its mission-critical applications in the event of a disaster. The BCP should include instructions necessary for recovery of business operations at an alternate site. Moreover, the BCP should be formally and periodically reviewed, tested to the degree possible, and approved.

- Ensure that the BCP includes detailed staff instructions to cover various disaster and recovery scenarios to ensure the continuity of business operations in the event of an unforeseen interruption. In addition, the BCP should include contingencies regarding staff, equipment, computers, or other resources for the alternate processing site.

- Clearly identify the overall disaster recovery strategy to be executed by EOHHS and ITD to assist MassHealth in regaining business operations. The BCP should identify specific IT-related processes or procedures that MassHealth staff may need to perform in the event of an emergency.

Auditee's Response

Regarding the Business Continuity Plan, the template provided to MassHealth from the Massachusetts Emergency Management Agency for the COOP Plans includes basic IT business continuity contingencies in the critical systems identification and dependencies on outside agencies/vendors section. Additionally, our expanded COOP includes the continuity of IT mission critical systems as well as the restoration of essential business functions at the departmental level and other operational elements typically included in a BCP. We believe the modifications to the content of our COOP serves the function of both a traditional COOP and BCP.