The Commonwealth of Massachusetts
AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
Boston, MASSACHUSETTS 02108
TEL. (617) 727-6200

No. 2008-0243-4T

OFFICE OF THE STATE AUDITOR'S REPORT
REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY–RELATED CONTROLS AT THE DEPARTMENT OF MENTAL HEALTH SOUTHEASTERN AREA OFFICE

July 1, 2007 through January 21, 2009

OFFICIAL AUDIT REPORT

JUNE 3, 2009

TABLE OF CONTENTS

INTRODUCTION

The Department of Mental Health (DMH) is organized under Chapter 19, Sections 1 to 21, of the Massachusetts General Laws and is placed within the purview of the Executive Office of Health and Human Services (EOHHS). The DMH is comprised of a central office and six area offices—DMH Central, Central Massachusetts Area, Metro Boston Area, Metro Suburban Office, North East Area, Southeastern Massachusetts, and Western Massachusetts—which operate within five regions. The DMH's primary mission is to set and maintain standards and regulations for the operation of mental health facilities and community residential programs throughout the Commonwealth. The DMH also provides clinical, rehabilitative, and supportive services for adults with mental illness, and children and adolescents with mental illness or emotional disturbance.

The DMH's Southeastern Area Office (SEAO) provides services to residents from 75 cities and towns in Barnstable, Bristol, Dukes, Norfolk, and Plymouth Counties. The Southeastern Area Office is comprised of an administrative office located in Brockton and seven regional offices located in Fall River, New Bedford, Taunton-Attleboro, Hyannis, Pocasset, Plymouth, and Brockton. At the time of our audit, the Southeastern Area Office had 41 employees, including four who were assigned to the SEAO from the DMH central office.

The SEAO's computer operations are supported through a local area network (LAN), consisting of a file server to which 32 workstations are connected throughout the SEAO administrative office and an additional nine workstations that are located at Taunton State Hospital. The file servers are connected to the Commonwealth's wide area network, referred to as MagNet, to provide access to DMH's Mental Health Information System (MHIS), the Massachusetts Management Accounting and Reporting System (MMARS), Human Resources Compensation Management System (HR/CMS), and other network services, including e-mail. In addition to the workstations available for SEAO personnel, the Office had six notebook computers that were assigned to senior managers. The SEAO receives technical support and guidance from DMH's Applied Information Technology Division.

The primary application used by SEAO to support its mission-critical business functions is the Mental Health Information System (MHIS) that was developed by a private vendor, MediTech Incorporated. MHIS provides automated processing for a variety of important client-related services. The SEAO uses the MHIS application to analyze and review admissions, medical records management, coding diagnosis, billing, accounts receivable, and accounts payable functions. MHIS is also used to monitor in-patient and out-patient medications. The MHIS application is supported through a cluster of file servers and application servers located at the Massachusetts Information Technology Center (MITC) in Chelsea. The

SEAO also utilizes Microsoft Office to perform various administrative functions, including the generation of statistical reports.

The Office of the State Auditor’s examination was limited to a review of certain IT general controls over and within the SEAO’s IT environment.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an examination of information technology (IT) general controls at the Department of Mental Health's Southeastern Area Office (SEAO). The audit, which was conducted from June 25, 2008 through January 21, 2009, covered the period of July 1, 2007 through January 21, 2009. The scope of our audit included an evaluation of IT-related controls pertaining to IT policies and procedures, physical security, environmental protection, system access security, inventory control of computer equipment, disaster recovery and business continuity planning, and provisions for on-site and off-site storage of backup copies of magnetic media. Our audit included a review of SEAO's awareness of the requirements of Executive Order 504 regarding the security and confidentiality of personal information.

Audit Objectives

Our primary objective was to determine whether IT-related controls were in place and in effect within the DMH's Southeastern Area Office to support a properly controlled IT processing environment. In this regard, we sought to determine whether the SEAO's IT-related internal control environment, including documented policies, procedures, and practices, provided reasonable assurance that IT control objectives would be achieved to support SEAO's business objectives.

We sought to determine whether adequate physical security controls were in place and in effect to prevent unauthorized access, damage to, or loss of IT-related assets at the SEAO's administrative office location as well as the satellite office located at Taunton State Hospital. We evaluated whether environmental controls provided adequate protection to ensure that processing capabilities would be safeguarded. With regard to inventory control of computer equipment, we determined whether an annual physical inventory was conducted, computer equipment was accurately reflected and accounted for in the inventory record, and that the inventory system of record was properly maintained. Regarding system access security, we sought to determine whether adequate controls had been implemented to provide reasonable assurance that only SEAO's authorized users were granted access privileges to the automated systems. We evaluated whether procedures were in place to prevent and detect unauthorized user access to automated systems through the microcomputer workstations connected to the local area network's (LAN) file server. In addition, we determined whether the SEAO was actively monitoring password administration and user account management.

We sought to determine whether an effective business continuity strategy, including user area plans, was in place that would provide reasonable assurance that mission-critical and essential IT-related operations could be regained within an acceptable period of time should a disaster render the computerized functions inoperable or inaccessible. We also sought to determine whether adequate procedures for on-site and off-site storage of backup media to support system and data recovery activities were in place. We determined whether appropriate user area contingency plans were in place to guide operational staff should external IT services be rendered inoperable for an extended period of time.

Audit Methodology

To determine the audit scope and objectives, we conducted pre-audit work that included obtaining and recording an understanding of relevant operations, performing a preliminary review and evaluation of certain IT-related internal controls, and interviewing senior management. To obtain an understanding of the IT internal control environment, we reviewed the SEAO's organizational structure and primary business functions, and identified the Office's IT infrastructure. We performed a high-level risk analysis for selected areas under our review, conducted a brainstorming session identifying areas of possible fraud and abuse, and assessed the strengths and weaknesses of the IT internal control system for selected activities. We also interviewed SEAO management regarding their approach to ensuring compliance with Chapter 93H of the General Laws and Executive Order 504 for the protection of personal information. Upon completion of our pre-audit work, we determined the scope and objectives of the audit.

Regarding our examination of controls pertaining to documented IT policies and procedures, we interviewed senior management from DMH and the SEAO and obtained and reviewed existing IT-related policies, standards, and procedures. For the selected IT areas under review, we assessed the extent to which existing documented policies and procedures addressed IT functions at SEAO.

To determine whether computer equipment was adequately safeguarded from damage or loss, we reviewed physical security over the computer room and file server room by interviewing senior management and security personnel and conducting walkthroughs. The file server room is located within SEAO's computer room. We confirmed the presence of physical security controls, such as locks and alarms, and determined whether access to the computer and file server rooms was restricted to only authorized personnel and adequately safeguarded. In addition, we conducted a site visit to the Taunton State Hospital facility that houses workstations for SEAO personnel to determine whether physical and environmental controls were in place over computer equipment.

To evaluate whether adequate environmental protection controls were in place to properly safeguard computer equipment and automated systems from loss or damage, we checked for the presence of fire detectors and alarms; fire suppression devices, such as sprinklers and hand-held extinguishers; power surge protectors; an uninterrupted power supply (UPS); and emergency lighting throughout the facility and administrative offices. We also reviewed general housekeeping procedures to determine whether only appropriate items were placed in the computer room and file server room. To determine whether proper temperature and humidity controls were in place, we reviewed for the presence of appropriate dedicated air conditioning units in the computer and file server rooms, the on-site storage location in Brockton, and the off-site storage location at Taunton State Hospital. We also reviewed control procedures to prevent and detect damage to automated systems and backup media that is stored on site and off site.

Concerning access security controls, we reviewed the DMH's Southeast Area Office's access security policies and procedures that are designed to prevent unauthorized access to the application systems and data files accessible through the SEAO's workstations. Our test of system access security controls included a review of access privileges for employees who were authorized to access MHIS and application systems residing on SEAO's file server. To determine whether system access security was being properly maintained through user account management and user ID and password administration, we compared the LAN and the MHIS system user lists provided by the DMH's Advanced Information Technology (AIT) to a roster of all 41 employees assigned to the SEAO. We reviewed a sample of completed authorization forms to determine whether there was documentary evidence that access privileges were authorized for system users. We determined whether procedures were in place to ensure that the security administrator was promptly and properly notified of changes in personnel status (e.g., employment termination, job transfer, leave of absence) and that user IDs and passwords were being promptly deactivated from the system or access privileges were being appropriately modified. We reviewed password administration controls, such as activation and deactivation, password length and composition, and the frequency of password changes.

To determine whether adequate controls were in place and in effect to properly account for the SEAO's computer equipment, we reviewed relevant inventory control procedures, obtained and tested the inventory record of computer equipment, and interviewed individuals responsible for inventory control. We reviewed the inventory record for the adequacy of data elements to identify, describe, and indicate the value, location, and condition of the equipment. We determined whether computer equipment was properly tagged with state identification numbers, and whether the serial numbers attached to the equipment were properly recorded on the hardware inventory listing. To determine whether the IT-related inventory record, dated October 30, 2008, was current, accurate, and valid, we tested 100% of the inventory consisting of 92 items of computer equipment located at SEAO's administrative office in Brockton and at the Taunton Hospital satellite office. To evaluate whether the system of record accurately reflected the items of computer equipment, we verified the location, description, inventory tags, and serial numbers of the hardware items listed on the inventory record to the actual equipment on hand.

To assess the adequacy of business continuity planning, we determined whether the SEAO, in conjunction with DMH, had developed formal disaster recovery or contingency plans for resuming computer operations should the network or computer systems be rendered inoperable or inaccessible. To assess the impact of a loss of processing capabilities, we conducted interviews with senior management to identify the impact on business functions provided at the SEAO that were supported by technology. In addition, we determined whether any user area plans had been developed specifically for the SEAO. To determine whether backup copies of application systems and data files would be available for the recovery of IT operations, we determined whether backup copies were generated on a scheduled basis and stored at secure on-site and off-site locations.

Our audit was conducted in accordance with generally accepted government auditing standards (GAGAS) issued by the Comptroller General of the United States and generally accepted industry practices. Audit criteria used in the audit included management policies and procedures and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT).

AUDIT CONCLUSION

Our audit of the Department of Mental Health's Southeast Area Office (SEAO) determined that adequate internal controls were in place and in effect to provide reasonable assurance that control objectives would be met for documented IT policies and procedures, environmental protection controls, system access security, inventory control of computer equipment, and on-site and off-site storage of backup copies of magnetic media. However, our examination found that controls needed to be strengthened for physical security over the computer and file server rooms, and for disaster recovery and business continuity planning for SEAO's computer operations.

Our review of IT internal controls found that the DMH's Advanced Information Technology had developed and documented policies and procedures for IT-related functions. We found that each system user was required to review and follow acceptable use policies outlined in DMH's "Security Handbook" and that the policies and procedures provided adequate guidance to SEAO staff in using technology to meet their responsibilities. We found SEAO management to be aware of the provisions of Executive Order 504 regarding the security and confidentiality of personal information and was in the process of implementing the requirements of the Executive Order into its internal control plan.

Our audit revealed that physical security controls over the SEAO computer and file server rooms needed to be strengthened to provide reasonable assurance that IT resources would be safeguarded from unauthorized access, use, or damage. Although DMH security personnel were present at the facility on a 24-hour, 7-days-a-week basis, and access to the computer and file server rooms was limited to authorized employees requiring a swipe card to gain access, our examination disclosed that installed motion detectors and intrusion alarms had not been activated to provide adequate protection for non-business hours.

Our examination of environmental protection over the computer and file server rooms revealed that appropriate controls were in place to provide reasonable assurance that IT resources were safeguarded from damage or loss resulting from environmental hazards. Specifically, adequate controls were in place to provide reasonable assurance that control objectives pertaining to air temperature; fire prevention, detection, and suppression; and emergency power and lighting would be met. We determined that there was an uninterruptible power supply for computer equipment in the server room to permit controlled shutdowns. However, we found that general housekeeping in the file server room needed to be improved, observing that the room was used for storage of supplies and contained excess clutter. Although SEAO took corrective action when this was brought to their attention, appropriate housekeeping procedures should be maintained for all areas housing computer equipment. Our examination of SEAO's satellite office at Taunton State Hospital confirmed that appropriate physical and environmental controls for computer equipment were in place and in effect.

Regarding system access security, we found that system access controls provided reasonable assurance that only authorized SEAO users had access to the LAN and the Mental Health Information System (MHIS). We found that administrative controls over user IDs and passwords provided reasonable assurance that access privileges would be deactivated, or appropriately modified, should SEAO employees terminate employment or incur a change in job responsibilities. In addition, the appropriate rules for password composition and frequency of change were in place for LAN and MHIS access. Our tests of user account management confirmed that all 41 current system users were authorized DMH or SEAO employees. However, our audit test of user accounts at SEAO's Taunton State Hospital office, conducted on November 21, 2008, found that one user who had left employment on November 14, 2008 still had access privileges. Once we informed SEAO management of the discrepancy, the user account was promptly deactivated.

With respect to inventory control of computer equipment, we found that SEAO was in compliance with the Office of the State Comptroller's fixed-assets policies and procedures' requirement that an annual physical inventory and reconciliation be conducted. In addition, we found that SEAO was maintaining an IT-related inventory on a perpetual basis in DMH's inventory system of record that included all required asset information with the exception of asset costs and dates of purchase or lease. Our audit test of the computer equipment inventory at SEAO disclosed that all items were locatable and had been tagged with assigned asset numbers. However, we believe that including the date of purchase or lease, asset condition, and cost for all computer equipment would enhance the computer equipment inventory record and support configuration management objectives.

Our audit disclosed that SEAO needed to strengthen business continuity planning in conjunction with DMH to be adequately protected against a prolonged loss of IT processing capabilities. At the time of our audit, sufficient instructions and guidelines were not documented to ensure that SEAO's business operations could be regained effectively. We believe that although DMH was aware of the need for disaster recovery and business continuity planning for IT operations and had begun to develop recovery strategies, further effort is needed to sufficiently develop comprehensive plans to address the needs of DMH area offices, including the SEAO. Our audit revealed that user area plans had not been established to document procedures to be followed by SEAO staff to support business continuity objectives in the event of a loss of IT operations. The loss of processing capabilities would impact the administrative functions performed by the SEAO. These functions include the processing of patient medication information, monitoring the availability of beds throughout the Southeastern Area, and billing for patient services. In addition, we determined that procedures regarding the generation of backup copies of magnetic media and the storage of the backup media at secure on-site and off-site locations were adequate.

AUDIT RESULTS

1. Physical Security Controls over the Computer Room and File Server Room

Our audit disclosed that, although we found certain physical security controls in place to safeguard IT resources and staff, physical security controls at the DMH's Southeastern Area Office's (SEAO) computer and file server rooms needed to be strengthened. Our audit revealed that access to the areas housing the microcomputer workstations, including all office areas, were limited to only authorized employees. We observed that the computer and file server rooms were found to be locked and required swipe key access. However, we found that the computer and server rooms were located on the ground floor in the rear of the building, adjacent to a rear parking area. We observed that the back wall and exit door were all glass with no safety or security mesh wire in place. In addition, we found that even though the computer room had been equipped with alarms and motion detectors, these devices had yet to be connected to provide adequate protection of IT resources.

According to SEAO management, budgetary constraints have limited its ability to select a vendor to connect these security devices and to install an alarm outside the glass wall and door. Even though the facility has building security provided by DMH on a 24/7 basis, the combination of non-functioning motion detectors and alarms as well as a glass exterior wall and entryway increases the risk of unauthorized access, damage to, or loss of IT equipment.

Generally accepted computer industry standards advocate the need for sufficient physical security controls to provide reasonable assurance that only authorized personnel have access to secure areas and that damage to, or loss of, IT-related assets will be detected and prevented. The absence of proper physical security controls places equipment and mission-critical data at risk of being lost or damaged.

Recommendation

We recommend that SEAO management strengthen physical security controls over the computer room and the server room by activating the motion detection equipment and intrusion alarms. We further recommend that SEAO management consider the installation of electrical sensors or metal bars for the windows and the door in the rear exterior wall. The sensors could be connected to the alarm system and would be activated to alert DMH security at the facility if the glass were broken and a security breech was in process.

Auditee's Response

> *The finding discussed with the Audit team on May 14 made note of some physical security weaknesses in the Computer Room area. As we discussed, the area directly accessible from the office door is used as an office area and is equipped with the same*

working equipment as any other office area in the building. This clarification is offered to further distinguish the Computer Room from the File Server room space that is further isolated and secured. The File Server room is the area in which the SE Area DMH servers are located. With this distinction agreed to, the recommended added security steps for the Computer Room will further enhance physical security and we do agree that further security considerations for the File Server room are appropriate.

We agree that at the time of the original visit, the Computer Room security was inadequate due to a malfunctioning locking system on the door. That door/locking system has since been repaired and the room is now secured with an appropriate locking system to which access is granted on a pre-authorized, need based policy. Access is limited to necessary AIT personnel, very limited facility and security personnel. DMH Area Facilities has begun a further review of the recommendations within the context of the Computer Room and are assessing further measures in the following areas:

- *Working with the Brockton Administration, there are plans to enhance the existing security system. Testing has already occurred which showed that the system is operational. Post the test we will be replacing and adding additional wiring. We will be activating features including motion detectors and door alarms. We also plan to add a feature onto the security system that will identify and trigger the alarm when a window is broken. In addition we plan to have a strobe light installed in the crisis area which is a 24/7 program that will notify the campus police in cases where the police were not in the IT server area.*

- *After the meeting in my office a request was made to Central Office Core Services Division to send an engineer to study the security and present physical set up of the IT room, both the outer IT office area and File Server room. We have requested funding to install metal bars inside the large window as well as further repair the security system for the Computer Room with hopes of expanding and enhancing the existing system. We would do this for all of the windows and rooms in this wing of the building.*

  Improved security on the server room will present a double lock situation for further protection to the servers and main SE Area files.

Auditor's Reply

We are pleased with the actions taken by SEAO management to strengthen physical security controls over the file server room by installing a double locking system and to continue to limit access to only authorized personnel. The additional measures to be taken will further strengthen physical security over the computer room and file server room. We encourage SEAO management to continue to pursue efforts to enhance controls, such as the installation of window alarms and motion detectors. We believe these actions will help reduce the risk of damage to or loss of IT-related equipment.

2. Disaster Recovery and Business Continuity Planning

Our audit revealed that, although the SEAO, in conjunction with the Department of Mental Health, had developed a draft business continuity plan, dated September 2007, and a Continuity of Operations Plan (COOP), dated August 2006, the SEAO did not have a sufficiently comprehensive business continuity plan and user area plans to guide staff to recover mission-critical business functions or implement appropriate contingency plans should IT systems be rendered inoperable for an extended period of time. We found that SEAO had implemented on-site storage of backup copies of magnetic media for data files residing on SEAO's file server and workstations and that DMH had established procedures for on-site and off-site storage of backup copies of magnetic media for MHIS. In addition, DMH had designated alternate processing sites for backup operations. However, a formal, comprehensive, and tested disaster recovery plan was not in place at the SEAO to provide reasonable assurance that SEAO's local area network-based systems and Microsoft Office Suite products can be recovered so that essential business operations can be regained effectively in a timely manner should a disaster render automated systems inoperable or inaccessible.

The SEAO utilizes the MHIS application system and the Microsoft Office Suite to support its mission-critical functions. The relative criticality of these automated systems needs to be assessed and the extent of potential risks and exposures to business operations needs to be documented. Although efforts have been made to address higher-level business continuity planning and recovery strategies for certain types of outages impacting DMH operations, sufficiently documented plans did not exist to provide adequate assurance that IT systems and related business operations at SEAO can be regained within an acceptable time period.

The loss of processing capabilities would impact the administrative functions performed by the SEAO for the patients throughout the 75 cites and towns that it services. Although SEAO does not have direct patient care responsibilities, the potential inability to regain processing capabilities would adversely impact SEAO's ability to process patient medications and determine the number of patients that could be serviced, since the availability of beds could not be readily determined. The SEAO's billing for patient services would be slowed, creating a possible delay in revenue collection or loss of revenue needed for operating purposes. Furthermore, management would be hindered from conducting any statistical analysis of patient activities in a timely manner.

The objective of business continuity planning is to help ensure the recovery and continuation of mission-critical and essential functions enabled by technology should a disaster cause significant disruption or loss of computer or network operations. Generally accepted industry practices and standards for computer operations support the need to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans.

Business contingency planning should be viewed as a process to be incorporated within the functions of the organization rather than as a project completed upon drafting a written plan. Since the criticality of systems may change, a process should be in place to identify a change in criticality or other factors, such as risk, and amend the business continuity and contingency plans accordingly. In addition, changes to the overall IT infrastructure and user requirements should be assessed in terms of their impact to existing disaster recovery and business continuity plans.

An effective disaster recovery plan should provide specific instructions to recover IT operations for various courses of action to address different types of disaster scenarios. Appropriate user area plans should outline recovery or contingency steps with detailed steps to be followed to efficiently restore business operations. The area plans should be coordinated with overall enterprise-based business continuity plans.

Recommendation

We recommend that SEAO assess its automated processing environment from a risk-management and business continuity perspective and further develop and test appropriate business continuity and contingency plans. We recommend that an assessment of criticality and business impact be performed at least annually, or upon major changes to SEAO's operations or the overall IT environment.

The business continuity plan should document SEAO's recovery and contingency strategies with respect to various disaster scenarios and outline any necessary contingencies. This plan should include a framework to establish minimum recovery requirements to maintain adequate business operations and service levels. The recovery plan should contain all pertinent information, including clear delineation of key personnel and their roles and responsibilities, needed to effectively and efficiently recover network or IT operations within the required time frames. We recommend that business continuity measures be tested and periodically reviewed and updated, as needed, to ensure the viability of the plans. SEAO's completed plans should be distributed to all appropriate staff who should be trained in the execution of emergency recovery plans. In addition, a complete copy of the plans should be stored in a secure off-site location.

Auditee's Response

> *After conferring with the IT Department, the Department of Mental Health has focused its Business Continuity Planning under the Office of Emergency Preparedness. Coop Plans, Pandemic Planning, IT Service Continuity Management, Site Business Continuity Planning are all efforts that are under review and assessment. In support of those efforts, DMH AIT has undertaken the formation of an Information Technology Infrastructure Library (ITIL) supported approach of emergency planning in the form of an Information Technology Service Continuity Management Plan. The plans for the implementation of that effort were shared with the Auditors at the exit interview. Since the audit began, progress has been made and a draft is under internal review. Further steps scheduled for the next few months are a complete criticality assessment for all business applications supported by DMH AIT and a comprehensive test plan. Once those tasks are complete, DMH AIT will present a draft plan for DMH Emergency Preparedness review and acceptance. Once we have passed that milestone, DMH will then share that draft with the Auditors for their further review and input if they would be willing to do so.*
>
> *Please note that with the Fiscal 2010 Budget that the IT function which has been Centralized within the Department will be shifted from the Department to a greater EHS IT Department. We will work with them as well to address the findings in the audit report. As noted in the report for the most part the SE Area can conduct its business on the IT platform from any location in DMH both within the Area and outside the Area. The major problem will occur when the statewide system experiences problems. We will defer to the plan noted above as our corrective action plan regarding the Department's Business Continuity Plan.*

Auditor's Reply

We acknowledge DMH's efforts in developing an Information Technology Service Continuity Management Plan. We are pleased that DMH will perform important procedures, such as performing a risk analysis and a criticality assessment for all business applications. Once the plan has been developed by DMH, appropriate SEAO staff should be trained to ensure that they could carry out their specific duties and meet their operational responsibilities should processing capabilities be rendered inoperable. Furthermore, the plan should be periodically tested to address any changes in processing or recovery requirements or any changes in technology that would impact recovery plans.