The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
Boston, MASSACHUSETTS 02108
TEL. (617) 727-6200

A. JOSEPH DeNUCCI
AUDITOR

No. 2009-0266-7T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE REVIEW OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE TAUNTON STATE HOSPITAL

July 1, 2007 through May 29, 2009

OFFICIAL AUDIT REPORT
JULY 10, 2009

TABLE OF CONTENTS

INTRODUCTION

The Taunton State Hospital (TSH) is governed by Chapter 19, Section 7 of the Massachusetts General Laws (MGL) and is administered by the Department of Mental Health's (DMH) Southeastern Area Office, under the guidance of the Executive Office of Health and Human Services (EOHHS). The Hospital, which is staffed by 512 employees, is managed by a Chief Operating Officer who supervises general administrative services and directs the primary organizational divisions, such as Clinical, Nursing, Professional, and Core Services. The Hospital, which is located in Taunton, Massachusetts, services the citizens of Southeastern Massachusetts including the Cape and Islands.

The primary mission of TSH is to provide comprehensive mental health and support services to improve the quality of life for adults and children with serious and persistent mental illness or severe emotional distress. The Hospital provides emergency evaluation and assessment, and intermediate-term and long-term inpatient care that includes forensic evaluations as required by the Massachusetts courts. The Hospital also provides treatment for adolescents, and rehabilitative and support services in a community setting. The TSH's inpatient units have the capacity to provide care and treatment for approximately 200 patients with serious mental disorders.

Regarding the IT environment, computer operations at the TSH are comprised of a local area network (LAN) that supports 379 microcomputer workstations. To collect important client-related information, the TSH utilizes the DMH statewide application systems, including the Mental Health Information System (MHIS) that resides on DMH servers located at the Massachusetts Information Technology Center (MITC) in Chelsea and the Pharmacy Information System that is operated by Tewksbury State Hospital. The MHIS application system provides financial information regarding client billings, accounts receivable, accounts payable, and electronic medical records, and the Pharmacy Information System supports order fulfillment of patient medications. Application systems that reside on IT servers located at Taunton State Hospital include the Infectious Disease Reporting, Investigations, Legal Guardianship, and Fixed Asset Tracking systems. In addition, the Hospital maintains a database to support the management of physical keys. The Commonwealth's WAN allows TSH to access the Human Resources/Compensation Management System (HR/CMS), and the Massachusetts Management Accounting and Reporting System (MMARS) applications that are operated at the Massachusetts Information Technology Center (MITC).

The Office of the State Auditor's review was limited to certain general controls over and within TSH's IT environment.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12 of the Massachusetts General Laws, we performed a follow-up audit of certain information technology controls at the Taunton State Hospital (TSH). Our audit, which was conducted from December 8, 2008 through May 29, 2009, covered the period July 1, 2007 through May 29, 2009. The scope of the audit consisted of an evaluation of the status of prior audit results in our IT audit report, No. 2005-0266-4T, issued June 28, 2005, pertaining to physical security controls and disaster recovery and business continuity planning. Our audit also included a review of logical access security and on-site storage of backup copies of magnetic media. Our audit included a review of TSH's awareness of the requirements of Executive Order 504 regarding the security and confidentiality of personal information.

Audit Objectives

Our primary audit objective was to determine whether TSH management had taken corrective action to resolve audit results regarding physical security controls and disaster recovery and business continuity planning identified in our prior IT audit report (No. 2005-0266-4T). We sought to determine whether adequate physical security controls were in place to restrict access to IT resources to authorized users only in order to prevent unauthorized use, damage to, or loss of IT-related equipment. Our objective regarding system access security was to determine whether appropriate administrative controls were in place to help ensure that only authorized personnel had access to the automated systems and that adequate password controls were being exercised.

We sought to determine whether adequate disaster recovery and business continuity plans were in place to provide reasonable assurance that computer functions would be regained within an acceptable period should a disaster render the TSH's computerized functions inoperable. In addition, we determined whether adequate on-site storage was being maintained for backup copies of mission-critical and important computer-related media.

Regarding the protection of personal information, we assessed the extent to which the Hospital was aware of the requirements of Executive Order 504.

Audit Methodology

To determine the audit areas to be examined during our IT audit, we reviewed the prior IT audit results regarding physical security and disaster recovery and business continuity planning that were documented in our prior IT audit report. We performed a high-level risk analysis, including areas of possible fraud and abuse, and assessed the strengths and weaknesses of the IT internal control system for selected activities. Upon completion of our pre-audit work, we determined the scope and objectives of the audit.

To determine whether computer equipment was adequately safeguarded from damage or loss, we reviewed physical security over the equipment by interviewing senior management and security personnel and conducting walkthroughs. To determine the adequacy of physical access controls, we confirmed the presence of physical security controls, such as locks and alarms, and determined whether access to the areas housing computer equipment was restricted to only authorized personnel. In addition, we reviewed the distribution, recordkeeping and return of keys used to access restricted areas.

Regarding logical access security, we reviewed documented policies and procedures that outlined the tasks to be performed to authorize, activate, and deactivate access privileges to application systems. To evaluate whether only authorized employees were granted access to the automated systems, we interviewed staff and obtained a system-generated user list from TSH of active user accounts. We then compared the list of user accounts to a current personnel listing. In addition, we conducted interviews of a limited sample of users to confirm job responsibilities and the level of system access granted to them. We reviewed control practices regarding logon ID and password administration by evaluating the extent of documented policies and guidance provided to the TSH personnel. We determined whether all employees authorized to access the automated systems were required to change their passwords periodically and, if so, the frequency of the changes.

To assess the adequacy of business continuity planning, we determined whether any formal planning had been performed to resume computer operations for systems residing at Taunton State Hospital and for addressing operational requirements for systems that are operated at MITC and at Tewksbury State Hospital. In addition, we determined whether the criticality of application systems used by the Hospital had been assessed, and whether risks and exposures to TSH's computer operations had been evaluated. Furthermore, to evaluate the adequacy of controls to ensure that copies of application and system software and data files residing at TSH would be available for recovering automated systems and network services, we interviewed DMH and Hospital staff regarding the generation and storage of backup copies of magnetic media. We observed the storage of backup media stored on site at the Hospital and reviewed procedures for off-site storage. We did not examine the off-site location where backup copies of magnetic media are stored.

To assess the extent to which the Hospital was aware of the requirements of Executive Order 504, we interviewed the Patient Information Officer who is responsible for helping to ensure that patient information is secured and kept confidential.

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 CONCLUSION

Our audit of the Taunton State Hospital (TSH) determined that adequate internal controls were in place and in effect to provide reasonable assurance that control objectives would be met for physical security, and were in place for logical access security and on-site storage of backup copies of magnetic media. However, we found that controls needed to be enhanced to adequately address disaster recovery and business continuity planning.

Regarding our examination of physical security, we found that corrective measures had been taken to address prior audit results to strengthen administrative controls over the distribution, recordkeeping, and return and collection of brass keys to improve security management. We found that TSH management has implemented policies and procedures that require all individuals who terminate their employment with the Hospital to return all access keys as a requirement of their exit procedure. We found that management has designated a point of accountability to maintain a security control plan for maintaining accountability of all keys and locks that are used by employees or contractors.

Regarding logical access security, we found that documented procedures for access security provided appropriate controls to grant system access privileges to users and to help ensure that appropriate password administration controls would be followed.

At the time of our audit, sufficient instructions and guidelines were not documented to ensure that IT systems operated at TSH to support business and medical functions could be regained effectively should the automated systems become inaccessible or inoperable. 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 develop sufficiently comprehensive plans to address the Hospital’s mission-critical and essential IT requirements. Our audit revealed that user area plans had not been established to document procedures to be followed by TSH staff to support business continuity objectives in the event of a loss of IT operations at TSH or from externally provided services. The loss of processing capabilities and readily available client-related data may adversely impact administrative and medical functions performed at the Hospital. These functions include the processing of client medication information, billing for client services, tracking and reporting of infection information, investigations and legal guardianship issues.

AUDIT RESULTS

Disaster Recovery and Business Continuity Planning

Although efforts have been initiated to develop business continuity plans at DMH facilities, our audit revealed that Taunton State Hospital (TSH) 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. Furthermore, we found that TSH management, in conjunction with DMH, had not assessed the relative criticality of their automated systems and determined the extent of potential risks and exposure to data processing operations. We found that TSH had implemented on-site storage of backup copies of magnetic media for data files residing on file servers and workstations and that DMH had established procedures for on-site and off-site storage of backup copies of magnetic media for the MHIS application. However, a formal, comprehensive and tested, disaster recovery plan was not in place at the TSH to provide reasonable assurance that the Hospital’s LAN-based systems could be recovered in a timely manner and that essential business and patient-related information can be regained effectively.

The Hospital uses the MHIS application system, the Pharmacy Information System, and their in-house application systems 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 high-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 TSH can be regained within an acceptable time period.

The loss of processing capabilities and readily available client-related information could adversely impact administrative and client services performed by the TSH. The potential inability to regain processing capabilities could adversely impact the processing of client medications, tracking and reporting of infectious disease information, and management of investigations and legal guardianship issues. Furthermore, the loss of processing capabilities could result in delays in billing for client services, creating a possible delay in revenue collection or loss of revenue needed for operating purposes.

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 TSH management, in conjunction with DMH, 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 TSH's operations or the overall IT environment.

We recommend that TSH obtain sufficient assurance that appropriate disaster recovery and business continuity plans are in place for externally provided IT services. We recommend that TSH perform a risk analysis and criticality assessment of all functional areas and business processes supported by technology and establish targets for acceptable time periods by which mission-critical IT operations and business functions need to be recovered. We recommend that the TSH document contingency and user area plans for automated systems that are not under the Hospital's control. We recommend that appropriate disaster recovery plans be developed for mission-critical and essential IT operations under the charge of the Hospital. Lastly, we recommend that the Hospital be involved in the development and review of recovery and contingency tests related to IT operations, and the approval of test results.

Auditee's Response

> *DMH 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 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. 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.*
>
> *As a Joint Commission accredited and CMS licensed facility, Taunton State Hospital conducts annual disaster drills to assure readiness for emergency events. The hospital has developed a Continuity of Operation Plans, ("COOP") which includes specific instructions for information management in the even of a catastrophic IT system failure. As noted in the audit report, the medical health information servers reside off-site and are backed-up every 24 hours. All on-site servers have back-up protocols where data is down-loaded to magnetic tape, stored in a fire-proof safe and transported weekly to Chelsea. Direct patient care is documented using down time procedures when there is a failure of the MHIS system. All of the TSH clinicians are trained and competent with the use of the down-time procedures. Nursing reference sheets are printed for each unit nightly for use during such episodes. Other crucial hospital business functions including MMRS, HR and payroll could be conducted from remote locations at other Southeast Area sites in the event of an IT outage specific to TSH. However, the hospital is awaiting the development of a centralized comprehensive DMH business continuity plan to assure that critical hospital functions can continue should IT systems be rendered inoperable for an extended period of time.*

<u>Auditor's Reply</u>

We acknowledge DMH AIT's efforts in developing draft documents for IT recovery plans. We reiterate our recommendation that TSH, in conjunction with DMH, 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 TSH's operations or the overall IT environment.

The business continuity plan should document TSH's recovery and contingency strategies with respect to various disaster scenarios and outline any necessary contingencies. The plan should include a framework to establish minimum recovery requirements to adequately maintain 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 be tested and periodically reviewed and updated, as needed, to ensure the viability of the plans, and 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.

APPENDIX

Status of Prior Audit Results

Control Area	Control Objective	Control Activities	Status of Control	Documented	Adequacy of Control
Physical Security over Access Keys	To ensure that adequate physical security controls are in effect to protect IT related assets from unauthorized access, use, damage or theft in areas housing IT equipment	Provide reasonable assurance that only authorized staff can access office areas and computer equipment to prevent loss or damage or unauthorized use.	Corrected	Policies regarding the distribution of brass keys for all secured areas at TSH is in place and in effect	Sufficient
Business Continuity Planning & Off-site storage	To determine whether business continuity controls would provide reasonable assurance that mission-critical and essential computer operations could be regained within an acceptable period of time should business functions be interrupted or seriously impacted.	Provide reasonable assurance that TSH can restore essential and mission-critical functions should automated systems be rendered inoperable.	Not fully corrected	Partial	DMH/TSH management needs to continue development of a comprehensive business continuity plan.

.