The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH

ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108

A. JOSEPH DeNUCCI
AUDITOR

TEL. (617) 727-6200

No. 2005-0266-4T

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

July 1, 2003 through March 15, 2005

OFFICIAL AUDIT REPORT

JUNE 28, 2005

2005-0266-4T

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 TSH, which is staffed by 512 employees, is managed by a Chief Operating Officer that supervises several functional components of general administrative services and directors of the major organizational divisions such as: Clinical, Nursing, Professional, and Core Services. The Hospital, which is located at 60 Hodges Avenue in Taunton, Massachusetts, occupies five buildings servicing the communities of: Taunton, Attleboro, Fall River, New Bedford, Brockton, Plymouth, Cape & Islands, along with surrounding areas.

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 required by the Massachusetts courts. The hospital also provides treatment for adolescents, and rehabilitative and support services in a community setting. The TSH inpatient units have the capacity to provide care and treatment for 187 patients with serious mental disorders.

Regarding the IT environment, computer operations at the TSH were comprised of a local area network (LAN) supported by four file servers to which 347 microcomputer workstations were connected. The file servers include one e-mail server, one application server, one Zero Administration Client (ZAK) server used to push out software updates to workstations within the Hospital, and a print server. To collect important client-related information, the TSH utilizes the DMH statewide applications, including the Mental Health Information System (MHIS) that resides on DMH servers located at the Massachusetts Information Technology Center (MITC); and the Pharmacy Information System (PIS) installed on a file server and administered by the Tewksbury State Hospital. The MHIS application provides financial information regarding client billings, accounts receivable, accounts payable, and electronic medical records, and the PIS application monitors patient medications. The Hospital’s microcomputer workstations are connected to the file servers housing the DMH statewide applications and the PIS at the Tewksbury State Hospital through the Commonwealth’s WAN. The Commonwealth’s WAN allows TSH access to the Human Resources/Compensation Management System (HR/CMS), and the Massachusetts Management Accounting and Reporting System (MMARS) applications through a group of file servers, located at the Massachusetts Information Technology Center (MITC) in Chelsea.

Our Office's examination focused on general controls for physical security and environmental protection, system access security, inventory control over IT-related resources, and business continuity planning, including on-site and off-site storage of magnetic media.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12 of the Massachusetts General Laws, we performed an audit of selected information technology (IT) related controls at the Taunton State Hospital (TSH) for the period covering July 1, 2003 through March 15, 2005. The scope of our IT audit included an evaluation of IT-related general controls at TSH. Areas reviewed included IT-related organization and management, physical security, environmental protection, logical access security, inventory controls over computer equipment, business continuity and contingency planning, and the on-site and off-site storage of backup copies of magnetic media. The audit was conducted from August 9, 2004 through March 15, 2005.

Audit Objectives

Our primary audit objective regarding the examination of IT-related controls was to determine whether TSH's IT environment was sufficiently controlled to support its automated systems and to safeguard IT-related assets. We sought to determine whether the IT-related internal control environment, including policies, procedures, and the organizational management structure provided reasonable assurance that IT-related control objectives would be achieved to support TSH's business objectives.

We evaluated whether adequate physical security and environmental protection controls were in place for areas housing computer equipment, to provide reasonable assurance that access would be available to only authorized users, and that damage to, or loss of computer equipment, software, and data files would be prevented and detected. The areas reviewed were the TSH's file server room, administrative offices, communication closets, and the on-site and off-site media storage location. A further objective was to determine whether adequate controls were in place to prevent unauthorized logical access to automated systems available through TSH's LAN.

Our objective regarding the proper accounting of IT-related assets was to evaluate that adequate controls were in place to provide reasonable assurance that computer equipment would be properly recorded in TSH's inventory record and accounted for and reported to the Office of the State Comptroller in accordance with laws and regulations.

We sought to determine whether an adequate business continuity and contingency plan was in place to provide reasonable assurance that computer and network capabilities could be regained to support data processing within an acceptable period of time, should a disaster render computerized functions inoperable or inaccessible. We did not review business continuity and contingency planning of the individual application systems because the applications do not reside on the Hospital's file servers.

These application systems are available through TSH's LAN but reside within MITC. We sought to determine whether adequate procedures were in place for on-site and off-site storage of LAN backup media to support system and data recovery operations.

Audit Methodology

To determine the audit scope and objectives, we conducted pre-audit work, which included obtaining and recording an understanding of the Hospital's mission and business objectives, relevant IT operations, reviewing and evaluating certain IT-related internal controls, and interviewing senior management from both TSH and the DMH Southeastern Area Office. In conjunction with our review of the internal control environment, we determined whether TSH, in conjunction with DMH, had developed, reviewed, approved, and implemented internal control documentation, including IT-related policies and procedures.

Regarding our examination of organization and management, we interviewed senior management, and obtained, reviewed, and analyzed existing IT-related policies, standards, procedures, as well as the TSH organizational structure. We also examined whether TSH had established a chain of command, appropriate span of control related to IT, adequate level of oversight, segregation of duties, and clear points of accountability. We sought to determine the level of IT strategic and tactical planning dealing with the Hospital's IT activity. We also reviewed job descriptions of IT personnel to gain an understanding of roles and responsibilities.

To evaluate physical security, we interviewed senior management and security personnel, conducted walkthroughs, and reviewed security logs. We also obtained a list of employees who had keys to the TSH file server room. Through observation we determined the adequacy of physical security controls, such as locks, visitor logs, motion detectors, and intrusion alarms. Regarding key management at the Hospital, we interviewed the Fire Marshal/Program Coordinator responsible for maintaining records of staff that were issued brass key sets and electronic keycards for the administrative offices within the building. Further, we interviewed the Fire Marshal/Program Coordinator regarding controls over the distribution and return of keys. We reviewed and evaluated written procedures regarding key management. In addition, to determine the adequacy of physical access controls regarding computer equipment located throughout TSH, we conducted site visits to the file server room, communication closets, office areas and to the on-site and off-site storage areas.

To evaluate whether adequate environmental protection controls were in place to properly safeguard automated systems from loss or damage, we checked for the presence of fire detectors and alarms, fire suppression methods, such as sprinklers and hand held extinguishers, power surge protection, uninterrupted power supply (UPS); emergency power generators, and emergency lighting in the file server room and the administrative offices. We reviewed general housekeeping procedures to determine

whether only appropriate items were placed in the file server room or in the vicinity of IT-related equipment. To determine whether proper temperature and humidity controls were in place, we reviewed for the presence of appropriate dedicated air-conditioning units in the file server room, and the on-site and off-site storage areas. We also reviewed control procedures to prevent and detect water damage to automated systems and IT-related backup media for on-site and off-site storage.

Our test of logical access security included a review of user accounts for individuals authorized to access TSH microcomputers and the client/server system. We determined whether logon ID and password access was established for authorized users employed by TSH. We determined the frequency that TSH staff was required to change their password to access the automated system. We compared the list of staff that were authorized to access the automated systems with the current TSH employee list, which included contract personnel, to determine whether all individuals who had access to automated systems were currently employed by TSH. We also reviewed password administration controls, such as granting passwords, requirements for length and composition of passwords, related security procedures, and the frequency of password changes.

To determine whether adequate controls were in place and in effect to properly account for TSH's computer equipment, we reviewed relevant inventory internal control procedures, obtained and tested the inventory record of computer equipment, and interviewed individuals responsible for inventory control. We determined whether computer equipment was properly tagged with state identification numbers and serial numbers and whether the serial numbers attached to the equipment were properly recorded on the hardware inventory listing. To assess the integrity of the information on the computer equipment inventory listing, we assessed the level of data completeness for all required data fields and accuracy for serial number, tag number, description, and location. To determine whether the IT-related inventory record, dated October 15, 2004, was current, accurate, complete, and valid, we tested a judgmental sample of 21 out of 351 workstations and file servers. We traced the state identification numbers for all 21 of the hardware items listed on the inventory list to the actual items on hand. In addition, we judgmentally selected an additional ten items of computer equipment and traced them from the physical location to the inventory record. Our audit did not include an examination of inventory controls for software.

To access the adequacy of business continuity planning, we reviewed disaster recovery and business continuity procedures documented by DMH's Central Area Office, for automated systems accessible through TSH's LAN. We interviewed management to determine whether the criticality of application systems had been assessed and whether risks and exposures to computer operations had been evaluated. To determine whether controls were adequate to ensure that IT operational information on TSH's file servers would be available should the automated systems be rendered inoperable, we interviewed DMH management responsible for creating backup copies of magnetic media at the Hospital. We reviewed the

adequacy of provisions for on-site and off-site storage for critical backup media and conducted a site visit to the off-site storage location to assess the adequacy of physical security and environmental protection. In addition, because our audit was limited to an examination of TSH control practices, we did not review the adequacy of on-site or off-site storage for DMH statewide applications processed on servers at the MITC.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and generally accepted computer industry control practices and auditing standards.

AUDIT CONCLUSION

Based on the results of our audit, IT internal controls in place at Taunton State Hospital provided reasonable assurance that control objectives related to IT organization and management, environmental protection, logical access security, and on-site and off-site backup copies of magnetic media would be met. However, our audit revealed that controls needed to be strengthened in the areas of physical security regarding electronic and brass key management, hardware inventory, and business continuity and contingency planning.

We found that controls related to IT organization and management provided reasonable assurance that IT administration control objectives would be met with respect to a well-defined IT organizational structure that provided an established chain of command, clear points of accountability and oversight of IT functions. IT management and staff were well aware of their responsibilities and IT-related job descriptions. Job specifications had been developed to reflect current responsibilities, and required technical knowledge and skills. Our review of IT-related planning found that the TSH and the Southeastern Area Office had developed written policies and procedures, as well as an IT strategic plan to support TSH's mission.

Our audit revealed that controls in place did not provide reasonable assurance that only authorized individuals could gain physical access to the Hospital campus. We found that for a significant number of individuals no longer employed by TSH, their brass key sets and keycards had not been turned into the Hospital. Employees used an electronic keycard system to gain access to the Hospital facility. The brass key sets were used to gain entry to specified rooms within TSH and to exit the Hospital. We determined that certain physical security controls were in place, including full-time security guards on duty 24x7 and an intrusion detection system for the entire Hospital facility. However, we determined that TSH needed to enhance policies and procedures related to physical security controls and to strengthen controls over the maintenance of brass key sets and the keycard access security system.

Our examination of environmental protection found that appropriate controls were in place to provide reasonable assurance that IT resources were operating in a proper environment to safeguard IT equipment and data files. Specifically, we found that control objectives related to general housekeeping, air conditioning, humidity control, fire prevention, detection, and suppression, emergency power and lighting, and power shutoff would be met for areas where the workstations and the file server room were located.

Our review of logical access security to the LAN's (Local Area Network) that provided access to networked applications, including the Mental Health Information System (MHIS) that supports administration and business operations, needed to be strengthened. We found that procedures were in

place to authorize and activate changes in access privileges. However, our test of authorized users to the LAN system revealed that procedures needed to be strengthened to ensure timely deactivation of access privileges for individuals no longer authorized or needing access to TSH's automated systems. We found that the security administrator was not being consistently notified in a timely manner of changes to access privileges. Our tests revealed that 29 former employees, some who had not been employed at the Hospital for up to two years, were found to be on the TSH LAN active user list. We recommend that the Hospital require department heads and the HRD to promptly notify the security administrator of changes in employee status that could warrant changes in access levels or complete deactivation of user privileges. Also, a periodic reconciliation of the LAN user access list to the current employee listing should be completed.

Our examination of inventory controls revealed that the Hospital and the DMH Southeastern Area Office needed to strengthen inventory controls to provide reasonable assurance that computer equipment was properly accounted for. Although TSH and DMH had developed policies and procedures regarding controls for fixed assets, including computer equipment, the policies and procedures need to be enhanced to ensure that inventory records are adequately maintained, monitored, and reconciled. With respect to the adequacy of the Hospital's system of record for computer equipment, our audit disclosed that the inventory record contained appropriate data fields, including date of acquisition, cost, location, identification tag, serial number, description, and condition. However, much of the information for the data fields regarding cost, date of acquisition, and condition was either incomplete or missing. The Hospital's inventory record would be strengthened by noting the asset's operational status such as being repaired, obsolete, or designated for surplus. Our review of TSH's inventory system, drawn from a judgmental sample of IT-related hardware, indicated that all items selected could be located, were in good condition, and were being utilized. We also determined that DMH's Southeastern Area Fiscal Division's Internal Control Manual requires TSH to maintain a perpetual inventory, verify the inventory on an annual basis, and reconcile the record to the Hospital's master inventory record. However, our audit tests revealed that TSH had not performed a physical inventory of its hardware items for over two years. In addition, the Internal Control Manual requires TSH to review items by a destruction committee in order to determine if the equipment is surplus or obsolete and disposable. However, the Hospital was unable to provide us with any record of IT-related equipment received or disposed of during the period of July 1, 2003 to March 15, 2005.

Regarding system availability, we found TSH had begun to formulate a business continuity strategy, in conjunction with the DMH Central Office. However, our audit indicated that the level of disaster recovery and business continuity and contingency planning needed to be strengthened. We found that there was a general absence of documented plans to address disaster recovery and business continuity

planning for automated operations. Our audit disclosed that TSH did not have a formal, tested, disaster recovery plan to provide reasonable assurance that mission-critical and essential data processing operations could be regained effectively in a timely manner, should a disaster render automated systems inoperable. We also found that although an alternate processing site had been identified, no user area plans had been established to document the procedures required to regain business operations in the event of a disaster. In addition, we determined that adequate procedures were in place regarding the storage of backup copies of magnetic media at secure on-site and off-site locations.

Auditee Response to Audit Conclusion:

The TSH IT Staff receives a bi-weekly staffing action report, which indicates which TSH employees have retired, transferred or terminated. This data allows the system administrators to deactivate system accounts in a more timely fashion if they are not contacted through the appropriate management and HR chain of command when such staffing actions occur. All department heads were notified by e-mail regarding the importance of notifying the LAN security administrator of all changes within their departments. The Department of Mental Health- Central Office- is in the process of filling a position to work on the Internal Controls of the whole Department. This will give us the opportunity to not only solidify our local controls but it will bring uniformity to Department wide controls. Administration is working on a process to assure an accurate physical inventory is conducted annually as per the Southeastern Area Fiscal Division's Internal Control Manual. Also, all descriptive information is being researched to add to the inventory database.

.

AUDIT RESULTS

1. Physical Security

At the time of our audit, although Taunton State Hospital did have certain physical security controls in place, controls needed to be strengthened with respect to electronic keycard and brass key management. We found that motion detector and magnetic contact door alarms were activated during non-business hours to prevent and detect unauthorized access to the hospital, and that intrusion alarms were installed to sound at the nearby police station. We determined that TSH had issued identification badges to everyone working within the TSH campus, and had in place a keycard security system for all three egress points throughout the Hospital's campus. We found that TSH management had established written physical security policies and procedures, including provisions for issuing and returning electronic keycard and brass key sets. However, although electronic keycards and brass key sets were originally issued to authorized TSH personnel, we found that since TSH had not set up appropriate monitoring controls, electronic keycards and brass key sets had not been returned by prior employees. We also determined that the unreturned electronic keycards had not been deactivated, nor had the brass key sets been re-keyed in order to prevent unauthorized physical access.

Our visual review of the Keri software system for electronic keycards revealed that there were currently over 1,600 keycards currently active on the system, with many users having duplicate cards. Although requested, we were unable to obtain a copy of the electronic keycard inventory from the Fire Marshall, who is the current administrator of the Keri software system. The administrator was unable to either print or save in electronic form the keycard inventory for our audit review, and as a result, we were unable to audit the current electronic keycard listing.

Our review of individuals holding brass key sets revealed that duplicate brass key sets had been issued and that a number of key sets had not been returned by individuals no longer employed by the Hospital. We determined that of the 902 issued brass key sets, 435 former TSH employees had brass key sets, representing an error rate of 48%. We also determined that of the 902 active brass key sets, 20 were undefined with no associated user name, representing an error rate of 2%. Furthermore, we found that 63 brass key sets were assigned to 30 current employees. Of these employees, 27 staff members had two brass key sets and three had three brass key sets assigned to them.

Our review disclosed that former employees still have custody of electronic keycards and brass key sets that, if used in combination, could provide access to areas housing microcomputer workstations. We also found that some former employees may still have access to the server room and the communication closets. As a result, the Hospital must enhance their physical security policies and procedures to more

adequately restrict physical access to only authorized individuals to prevent loss, damage, or theft of IT resources housed in various Hospital locations.

Generally accepted computer industry practices indicate that appropriate physical security controls should be in place to ensure that the information technology assets are operating in a safe and secure operating processing environment and that IT-related resources be protected from unauthorized access, use, damage, or theft. Those control measures need to include preventive controls, such as authorization, locked areas, identification and authentication, and detective controls, such as intrusion detection and alarms. Both the review of brass key sets and the electronic keycard system rely on certain elements of authentication. By more closely administering the validity of electronic keycard and brass key set access, the Hospital will strengthen its authentication controls in this area.

Recommendation:

We recommend an immediate reconciliation of the brass key sets and electronic keycards to current employees to ensure that appropriate access privileges have been granted. We also recommend that the Hospital consider re-keying locks to designated secure areas. We recommend that TSH enhance the documented procedures for managing the keycard access system and the brass key sets. The procedures should include requirements that prompt notification be made to Fire Marshall of all required changes in security access, including transfers of staff to other DMH facilities and terminations of employment, as well as prompt notification of lost or stolen keycards and brass key sets to enable timely deactivation. The procedures should also require periodic reconciliation of the active access cards and brass key sets to current employees to identify any cards requiring deactivation. We recommend that individuals be assigned only one access card. However, if individuals are required to have brass key sets, we recommend that generic group sets for brass key sets not be used. We recommend that the TSH consider retrieving all brass key sets designated as "undefined" and reissue them on an as needed and authorized basis with an appropriate time limit.

Auditee's Response:

> *The Fire Marshal is currently deactivating 5 electronic keycards per week. If there is no request for reactivation, the keycard access is eliminated. The process will be complete by July 31, 2005.*
>
> *Our current protocol requires the Human Resources Department to notify the Fire Marshal when an employee is being hired or terminated. Administration will be sharing the audit results and review current protocol with department heads and senior staff in an effort to convey the seriousness of key control and remind them of their role.*

It is essential an electronic report be generated to monitor the keycard database. Upon receipt of an upgraded 80-gb hard drive computer and a printer, the Fire Marshal will be able to download the free software available from the manufacturer. This will enhance the facility's ability to create reports to monitor and control the keycard access.

The Fire Marshal has also begun working with other agencies that occupy space at our facility to account for both the brass keys and the keycards. He has provided identifying tags that are agency specific to each group. He has also deactivated current keycards and issued new keycards in order to get an accurate count of what has been issued to each group.

The Fire Marshal will begin removing all locks that respond to the #75 key and replacing them with a TE key. This task will be complete by July 31, 2005. The results of this change will be monitored for 6 months beginning August 1, 2005. This change will effectively secure all inpatient units. It will also affect many areas that currently house PC's. We anticipate this change will positively affect our ability to control access to many areas in this facility. This committee will meet again in December to discuss our need for further re-keying to continue meeting the security control issues.

A thorough review of Operational Protocol SAT-EC-025 titled "Key and Electronic Access Control Program" revealed the need for a periodic reconciliation process. It was determined that the Fire Marshal and his designees will conduct a random inspection of employee keys monthly. This inspection will involve no fewer than 10% of TSH.

Also added to the protocol, is the requirement for new staff to sign a statement signifying their agreement to follow the procedures listed in order to ensure a more secure system. All staff will also be required to sign for all keys issued.

E-mail was sent to all staff regarding 'Loaner Keys'. This e-mail addressed the necessary security issues and specific instructions to employees. This topic is also on the agenda for the Sr. Management meeting to be held on Thursday, June 30, 2005. A copy of this e-mail will be included with the above-mentioned protocol as an attachment.

The Fire Marshal has secured all generic key sets. It is the expectation of this Administration that employees have only 1 set of keys. To that end, once a keycard is reported missing, it will be deactivated before a new keycard is issued. Also, Department heads will be charged with the task of assuring every effort has been made to locate the missing brass key set.

Auditor's Reply:

We commend the Hospital for the corrective measures taken to improve physical security by developing and implementing the recommended policies and procedures regarding keycard access and brass key sets. The Hospital should ensure that appropriate assurance procedures are in place to sufficiently monitor compliance with the established security requirements and standards.

2. Business Continuity and Contingency Planning

Although efforts were underway to develop business continuity plans at DMH facilities at the time of our audit, Taunton State Hospital's business continuity plan had not been completed to provide reasonable assurance that business functions supported by technology could be effectively regained in a timely manner. Although the Hospital has taken efforts to back up the LAN file servers, a determination of critical and essential backup copies of application systems and data files needs to be made. Specific arrangements need to be made to provide for an alternate processing site. We found that there was no formal agreement in place with another organization for alternate-site processing should the LAN be unusable or inaccessible. Further, TSH had not assessed the relative criticality of their automated systems to determine the extent of potential risks and exposure to data processing operations. Our audit also revealed that system users had not developed user-area contingency plans to address a potential loss of their automated processing. Without adequate disaster recovery and contingency planning, including required user-area plans, TSH was at risk of not being able to gain access to automated systems. A loss of processing capabilities could adversely affect both medical and business functions. Furthermore, the absence of a comprehensive and tested disaster recovery plan could result in unnecessary costs and significant processing delays.

Disaster recovery and business continuity plans should be well tested to reduce time and the risk of errors and omissions when restoring computer operations. An effective disaster recovery plan should provide specific instructions for various courses of action to address different types of disaster scenarios. The plan should identify the ways in which essential services would be provided without full use of the data processing facility, and the manner and order in which processing resources would be restored or replaced. The plan should identify the policies and procedures to be followed, detailing the logical order for restoring critical data processing functions, either at the original site or at an alternate-processing site. In addition, the plan should describe the tasks and responsibilities necessary to transfer and safeguard backup copies of data files, program software, and system documentation from off-site storage to the site being used for restoration efforts.

Sound management practices, as well as industry and government standards, advocate the need for a comprehensive and effective backup and disaster recovery and business continuity plan. Contingency planning should be viewed as a process to be incorporated within the functions of the organization, rather than as a project completed upon the drafting of a written plan. Since the criticality of systems may change, a process should be in place that would identify a change in criticality and amend the contingency

plans accordingly. System modifications, changes to equipment configurations, and user requirements should be assessed in terms of their impact to existing disaster recovery and contingency plans.

Recommendation:

The Hospital should assess the criticality of automated systems to identify application priorities and critical resources. An analysis should be conducted to identify risks and exposures relating to the TSH's data processing operations and microcomputer environment. The Hospital should identify potential processing alternatives and resources to be utilized should a disaster disrupt its data processing or business operations. Based upon these results, and input solicited from management and user departments, a written disaster recovery and business continuity plan should be developed. The plan should then be reviewed and tested, to the extent possible, approved by senior management, and implemented.

We further recommend that TSH, in conjunction with DMH's Southeastern Area Office, develop procedures to ensure that the criticality of systems be periodically reassessed, that the impact of changes in user needs or automated systems be evaluated, and that staff be adequately trained in executing recovery plans. Upon a major change to systems or equipment, or at least annually, the disaster recovery plan should be reviewed, updated, and tested to ensure that it is current, accurate, and complete. The business continuity plan, or specific sections of it, should be distributed to appropriate personnel, and a complete copy of the plan should be stored in a secure off-site location.

Auditee's Response:

> *We would like to clarify that DMH does have a Business Continuity Committee and that someone from the TSH IT staff does act as a member. We provided all of our agendas and minutes of those meetings for the past year. In addition, DMH had developed a draft IT business continuity plan and is working on a disaster recovery plan. We will work to test this plan with facility staff, IT staff and vendors as soon as possible. We will be working to document our procedures for business functions and clinical system function contingency planning with regard to IT. Many informal plans are in place. For example, any DMH TSH business user can work in a nearby DMH Southeast Area facility and complete the same day-to-day MMARS, HR/CMS tasks. The TSH hospital staff does have electronic access to patient face sheets and critical assessments on any ward, if the MHIS system is not accessible at any given time. This is part of our business continuity planning system.*
>
> *In an effort to further assess the IT vulnerability at TSH, DMH had a vendor, VeriSign, come into the facility and perform a HIPAA Security Risk Assessment, including an extensive facility walk through, procedure/policy review and system/LAN vulnerability scan. This work was done within the past 30-60 days. We expect to receive a report on*

those findings and work to remediate the risk that has been addressed in this audit as well as by our HIPAA Security Risk Assessment.

Auditor's Reply:

We acknowledge that the Hospital is aware of the need for business continuity planning for its mission-critical and essential application systems. However, we urge TSH management to work toward developing a comprehensive business continuity plan. We recommend that recovery plans and procedures be established to address business continuity planning. Once the plan is developed, it should be tested to assess its viability and periodically reviewed and updated as necessary. This is especially important since the Hospital relies on information technology in performing its primary business functions.