A. JOSEPH DeNUCCI
AUDITOR

The Commonwealth of Massachusetts

AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL. (617) 727-6200

NO. 2007-0270-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY AND FINANCIAL-RELATED CONTROLS AT THE WRENTHAM DEVELOPMENTAL CENTER

March 1, 2005 through February 9, 2007

OFFICIAL AUDIT REPORT

JUNE 25, 2007

TABLE OF CONTENTS

INTRODUCTION

The Wrentham Developmental Center (WDC), which began operations in 1907, is governed by Chapter 19B, of the Massachusetts General Laws (MGL) and is placed organizationally under the Department of Mental Retardation (DMR). The Executive Office of Health and Human Services (EOHHS) provides additional oversight and guidance for WDC's IT operations, functions, and activities. The WDC, which is located on more than 400 acres of farm and wooded lands in Wrentham, Massachusetts is an intermediate care facility that provides residential care for approximately 300 developmentally impaired adults. The WDC accommodates and medically assists clients in three units encompassing 17 residences and a 12-bed acute care medical center. At the time of our audit, the WDC was staffed by approximately 900 employees. The WDC received $44,608,631 of state funds for fiscal year 2005 and $44,631,144 for fiscal year 2006.

The WDC uses information technology to carry out its mission and support its business operations. The WDC does not have its own IT Department, but relies on DMR to manage and support its IT operations. In this regard, DMR has assigned a site manager to support the daily WDC computer operations. The WDC's computer operations are supported through the use of a LAN, which consists of one file server connecting 221 microcomputer workstations throughout the facility. The LAN provides connectivity through telecommunication lines to two file servers at the DMR central office in Boston and the Commonwealth's wide area network (WAN). The primary application systems used at the WDC include the Home and Community Services Information System (HCSIS) and the MediTech application system that are used to process a variety of administrative and medical information, pertaining to patient admissions and discharges, client records and investigations. The LAN supports word processing products and uses 13 of the microcomputer workstations for training purposes. The HCSIS is a DMR web-based application that provides incident collection and reporting of information pertaining to WDC's clients. The MediTech application was developed by a private vendor, and implemented by the Bureau of Hospital Management. The application supports the WDC mission by providing automated processing information for admissions, medical records, coding diagnosis, therapeutic information, patient care billing and accounts receivable. The MediTech application is supported through a group of file servers located at the Massachusetts Information Technology Center in Chelsea, Massachusetts and is technically supported by Meditech Inc.

The Office of the State Auditor's examination was limited to an examination of certain IT general controls over and within WDC's IT environment and a review of selected financial-related controls.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

From July 17, 2006 through February 9, 2007 we performed an audit of selected information technology (IT) and financial-related controls at the Wrentham Developmental Center (WDC) for the period covering March 1, 2005 through February 9, 2007. The scope of our audit included an evaluation of IT-related controls pertaining to documented IT-related policies and procedures, physical security, environmental protection, system access security, inventory control over computer equipment, disaster recovery and business continuity planning, and on-site and off-site storage of backup copies of magnetic media.

Our audit scope also included a review of financial-related controls pertaining to documented policies and procedures over non-Medicaid patient billing. We also examined the controls over the security and retention of confidential hardcopy medical records and the current status of nursing licenses at the WDC.

Audit Objectives

The primary audit objective regarding the examination of IT-related controls was to determine whether the IT environment was sufficiently controlled to support WDC's automated systems and to safeguard computer equipment. We sought to determine whether the IT-related internal control environment, including documented policies and procedures, provided reasonable assurance that IT control objectives would be achieved to support the WDC's mission.

We sought to determine whether adequate physical security and environmental protection controls were in place to protect residents and staff, and to safeguard computer equipment. The areas reviewed housing computer equipment were the WDC's administrative offices, buildings housing residential units, file server room, and the on-site and off-site storage locations for the backup media. We sought to determine whether adequate controls were in place to prevent unauthorized access to data and systems residing on WDC's workstations.

Regarding inventory control, we sought to determine whether adequate controls were in place and in effect to provide reasonable assurance that computer equipment was properly recorded, accounted for, and safeguarded against unauthorized use, theft, or damage. Regarding system availability, we sought to determine whether adequate controls were in place to provide reasonable assurance that on-site and off-site storage of backup copies of magnetic media were in place to assist recovery efforts. We sought to establish whether IT operations could be regained within an acceptable period of time through a comprehensive business continuity strategy should IT systems be rendered inoperable or inaccessible. In conjunction with reviewing business continuity planning, we determined whether proper backup

procedures were being performed and whether copies of backup magnetic media were stored in secure on-site and off-site locations.

Regarding our examination of financial-related controls, we sought to determine whether adequate documented policies and procedures were in place to review direct care patient charges not billed to Medicare and the formal recording and reconciling of these charges. A further objective was to determine whether controls were in place for the security and retention of confidential hardcopy medical records maintained at the Center. We also sought to determine whether all nursing staff employed at the Center had valid, up-to-date nursing licenses on record with the Massachusetts Division of Professional Licensure.

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 internal control environment, we reviewed the DMR and EOHHS IT organizational structures and relevant WDC staff and primary business functions. We performed a high-level risk analysis and assessed the strengths and weaknesses of the internal control system for selected IT and financial-related activities and determined the scope and objectives of the audit upon completion of our pre-audit work.

Regarding our examination of controls pertaining to documented IT policies and procedures, we interviewed senior management from both the DMR and WDC, and obtained and reviewed existing IT-related policies, standards, and procedures. For selected IT functions, we assessed the extent to which existing documented policies and procedures addressed the IT functions. We also reviewed the degree of oversight provided by DMR and EOHHS to support WDC's IT functions.

To evaluate physical security, we interviewed management, conducted a walk-through of areas housing IT equipment, such as resident units, file server room and administrative offices. Through observation and tests, we determined the adequacy of physical security controls over areas housing IT equipment. We examined the existence of controls such as office door locks and intrusion alarms. We determined whether individuals identified as being authorized to access areas housing computer equipment were current employees of WDC or DMR and that these areas were restricted to only authorized personnel. Further, we reviewed procedures to document and address security violations and/or incidents and requested a list of key holders to areas housing computer equipment.

To assess the adequacy of environmental protection controls, we interviewed management, conducted walk-throughs of areas housing IT equipment, such as buildings housing residential units, file server room, on-site and off-site storage areas for backup copies of WDC's magnetic media and administrative

offices. To determine whether adequate environmental protection controls were in place to protect IT resources, we examined general housekeeping; fire prevention, detection, and suppression; heat detection; uninterruptible power supply; emergency lighting and shutdown procedures; water detection; and humidity control and air conditioning. Audit evidence was obtained through interviews, observations, and a review of relevant documentation.

To determine whether adequate controls were in place and in effect to properly account for WDC's computer equipment, we reviewed inventory control policies and procedures, interviewed individuals responsible for inventory control, and obtained and tested the inventory record of computer equipment. With regard to inventory control over IT equipment, we evaluated whether an annual physical inventory was conducted, whether IT equipment was accurately reflected in the inventory system of record, and whether the IT system of record was properly maintained. We examined policies and procedures regarding fixed-asset inventory to determine whether the WDC was in compliance with the Office of the State Comptroller's regulations regarding conducting an annual physical inventory and reconciliation. We evaluated the integrity of the system of record for computer equipment initially provided by DMR's site manager for WDC and then updated by DMR central office. We reviewed the inventory records to determine whether the lists contained appropriate data fields to identify, describe, and indicate the value, location, and condition of computer equipment including fields of information for acquisition dates, condition, identification tag numbers, location, descriptions, and historical costs. To determine whether the system of record for computer equipment was current, accurate, and valid, we initially tested a judgmental sample of 76 out of 486 IT-related items listed on the WDC inventory list provided by the DMR site manager dated August 16, 2006. Additionally, we also judgmentally selected an additional 39 items observed during our walk-through of the Center and traced them to the inventory listing.

To determine whether the official system of record provided by DMR on December 14, 2006 was current, accurate and valid, we used Audit Command Language (ACL) software to select a statistical sample of 106 items out of a total population of 437 items in order to achieve a 98% confidence level. We examined the inventory record for acquisition dates, condition, identification tag numbers, location, and description.

To obtain an understanding of access security controls, we reviewed the DMR's access security policies and procedures that would provide reasonable assurance that only authorized users had access to the systems and to prevent unauthorized access to WDC's applications systems and data files accessible through the workstations. Our test of system access security controls included a review of user accounts for all WDC employees and consultants who were authorized to access WDC and DMR application systems. We also reviewed job descriptions for individuals possessing supervisory levels of access. To determine whether system access security was being properly maintained through the management of user

IDs and passwords, we compared the system user list provided by the WDC to a roster of all WDC employees and consultants. We also reviewed password administration controls, such as activation and deactivation, password length and composition, and the frequency of password changes.

To assess the adequacy of system availability, we determined whether formal planning had been performed to develop and maintain a business continuity plan to resume computer operations should the network application systems be inoperable or inaccessible. We also determined whether the criticality of application systems had been assessed, and whether risks and exposures to computer operations had been evaluated. To evaluate the adequacy of controls to protect data files through the backup of on-site and off-site magnetic media and hardcopy files, we interviewed WDC staff regarding the generation of backup copies of computer-related media.

To determine whether adequate documented policies and procedures were in place to record and reconcile patient charges, we reviewed relevant policies and procedures, and conducted interviews with WDC and DMR management. The total annual billing amounts for fiscal year 2006 was $1,780,216. We reviewed the billing transactions for the month of August 2006 totaling $139, 033 to verify that proper procedures for patient charges billed directly by WDC were being properly accounted for, recorded and reconciled in WDC's accounting records.

To verify whether adequate controls were in place to safeguard confidential hardcopy client records, we examined policies and procedures and conducted interviews with WDC employees. Further we conducted a walkthrough and identified the presence of physical security and environmental controls such as secure location with intrusion alarms and locked doors, fire detection, prevention, and suppression devices for the areas used to store the confidential records.

To determine whether all nursing staff employed at the WDC had current and valid nursing licenses, we verified the status of 90 (100%) licenses with the Massachusetts Division of Professional Licensure.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by 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) as issued by the Information Systems Audit and Control Association in July 2000.

AUDIT CONCLUSION

Based on our audit at the Wrentham Development Center, we determined that internal controls in place provided reasonable assurance that IT-related control objectives pertaining to environmental protection for areas housing IT equipment and on-site and off-site backup of computer media would be met. However our audit revealed that controls pertaining to organization and management, physical security, environmental protection for the area housing historical hardcopy client records, system access security, inventory control over computer equipment, and business continuity planning needed to be strengthened. Our review of financial-related controls revealed weaknesses in the billing procedures utilized by the WDC in conjunction with the Department of Mental Retardation.

Our examination of documented IT policies and procedures indicated that the WDC in conjunction with EOHHS and DMR had only limited formal documentation that was not sufficiently comprehensive to address WDC IT operations. Specifically, we found that IT-related policies had not been updated to reflect the technology changes at the WDC and staff were not certain about responsibilities for IT activities. We found that policies and procedures regarding physical security, environmental protection, inventory control over computer equipment, on-site and off-site storage of backup computer media and disaster recovery and business continuity planning do not reflect the current IT environment.

Our audit revealed that adequate physical security controls were in place over the file server room and administrative office areas, except for the management of keys to client living areas. We found that authorized access to the server room was limited to four WDC senior management personnel. Further, our audit revealed that security personnel were stationed at the WDC to monitor activities on a 24-hour basis. However our examination revealed that controls over the management of keys to areas housing residents must be strengthened. We found that WDC management did not maintain a list of key holders for areas housing both computer equipment and residents throughout the facility and, therefore, could not be assured that access would only be limited to authorized staff.

Our examination of environmental protection over the office area and file server room concluded that the WDC had appropriate control mechanisms in place to provide reasonable assurance that IT resources were being protected. Specifically, we found that control objectives related to general housekeeping; air conditioning; fire prevention, detection, and suppression; emergency power and lighting; and emergency shut down would be met. We observed the file server room had strong environmental controls to protect personnel and equipment. However, our audit revealed that the building designated to store confidential personal and medical records of former clients had serious environmental deficiencies. We found that

the building did not contain automatic fire suppression equipment and, as a result, these records were at risk of being damaged or destroyed in case of a fire.

Our review of system access security for the application systems that provide mission critical information such as processing for admissions medical records information, coding diagnosis, therapeutic information, patient care, billing, accounts receivable and electronic medical records, needed to be strengthened. Our review of password administration indicated that employees were required to change passwords every 90 days for both the HCSIS and MediTech systems and requirements for composition of passwords was adequate. However, regarding our tests of authorized users of the HCSIS application system, we found that 26 out of 409 users could not be identified as current employees on the August 7, 2006 payroll record. Our test of authorized users of the MediTech application system indicated that four out of 313 users could not be identified on the December 15, 2006 payroll record. Our examination further revealed that these unidentified authorized users were former or retired employees having termination dates back to June 2004. Our tests of individuals possessing supervisory level access indicated that access levels were appropriate when compared to job descriptions.

Our audit revealed that DMR could not provide reasonable assurance that the system of record for computer equipment, could be relied upon, since a complete annual physical inventory and reconciliation was not being performed to assist in verifying the accuracy and completeness of the inventory record. Our audit revealed that there were two IT-related inventories being maintained for computer equipment at the WDC. Our audit tests revealed that at the initiation of our audit, WDC management in conjunction with DMR could not provide a comprehensive inventory listing of computer equipment. We found that during the course of our audit an inventory listing was developed by DMR's site manager at WDC for computer equipment at the facility. This inventory list, dated August 16, 2006, consisted of 486 computer equipment items. A second inventory listing, dated December 14, 2006, consisting of 437 IT-related items was generated by DMR central office and deemed to be the system of record. We compared both inventory records and determined that the master record did not account for 49 IT-related items at the WDC. Our examination revealed these items were microcomputers used by WDC for training and as spare equipment. Our audit test of selected assets from both lists revealed that all items were located and properly tagged. However, we found that neither list contained informational attributes, such as acquisition dates, historical costs, installation dates and condition of the equipment. The absence of a reliable comprehensive inventory and reconciliation of computer equipment hinders WDC's and DMR's ability to properly account for IT resources, evaluate the allocation of equipment, identify missing equipment, and meet IT configuration objectives.

Regarding system availability, 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 WDC and DMR 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 or inaccessible. 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. We did determine 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.

Regarding our review of policies and procedures related to patient billing for non-Medicaid services and charges for care at WDC, we found limited procedures in place. Moreover, we determined that WDC did not have comprehensive, written, and approved billing policies and procedures in place and in effect for non-Medicaid services and charges. Although we only reviewed the August 2006 billing information and spreadsheets that were prepared for patient charges for care, WDC could not provide sufficient documentation that they had reconciled monthly billing amounts for fiscal year 2006 and the first four months of fiscal year 2007. We recommend that WDC, in conjunction with DMR, develop and implement policies and procedures to account for and monitor patient billing for non-Medicaid services and charges.

Our examination of the security and retention of confidential records indicated that the WDC had established policies with regard to maintenance of these records, but the areas designated for storage did not have adequate environmental controls. We found that the WDC retains all original hardcopy client information and the personal records being maintained include medical, financial, and personal history information. Regarding environmental controls, we observed that there were serious deficiencies in the building designated by WDC management to store hardcopy confidential personal and medical records. Should these records be damaged or destroyed, family members and health care providers could be denied access to important personal, financial, and medical history information. Our audit revealed that there was no automatic fire suppression equipment in any area of the storage building. We believe that management had not fully assessed the risk of the impact of losing vital historical information should they be damaged or destroyed. The WDC should consider either moving these records to an environmentally sound facility or consider the use of fireproof cabinets until a permanent resolution to the proper storage of these records can be established.

Our examination of all nurses employed by the WDC revealed that each nurse held a current and valid license in compliance with the Massachusetts Division of Professional Licensure.

AUDIT RESULTS

1. Documentation of IT-related Policies and Procedures

Our audit revealed that Wrentham Developmental Center (WDC), in conjunction with DMR and EOHHS, needs to strengthen and update policies and procedures to ensure that the staff has sufficient guidance for performing IT-related functions. At the time of our audit, the WDC did not have updated policies and procedures in place to adequately address the current information technology environment and to provide reasonable assurance that control objectives would be achieved for physical security, system access security, environmental protection, inventory control over computer equipment, and business continuity planning.

Formal documentation of IT-related policies and procedures provides a good basis for ensuring that desired actions are taken and that undesired events are prevented or detected and, if detected, that corrective action is taken in a timely manner. Documented policies and procedures also assist management in training staff, serve as a good basis for evaluation, and increase communication among personnel to improve operating efficiency and effectiveness. Clearly, well-trained personnel develop a better understanding of their duties and improve their levels of competence when documented procedures are followed. The absence of current documented policies and procedures may lead employees to rely on individual interpretations of what is required to perform required IT-related functions. In such circumstances, management may not be adequately assured that desired actions will be taken. In addition, Chapter 647 of the Acts and Resolves of 1989 requires that all state agencies have documented and approved internal control policies and procedures.

The lack of formal documented policies and procedures limits DMR's ability to provide guidance and oversight for IT activities at the Center. Documentation of key processes and activities within IT functions help to provide clear guidelines regarding the exercise of control practices and monitoring and evaluation of expected results. Documented policies and procedures should address all IT functions, including IT planning, risk assessment, risk management, defining information architectures, data ownership, security, virus protection, authorized use of IT resources, training, monitoring, and reporting. The inability of DMR to provide WDC management with documentation for IT policies, procedures, and internal controls results may result in inadequate accountability, noncompliance with applicable laws and regulations, and improper resource management.

Recommendation:

DMR in conjunction with WDC management should develop, document, and promulgate policies and procedures to control IT-related activities, including the areas of IT-related organization and management,

physical security and environmental protection over IT resources, inventory control over fixed assets, including computer equipment, and disaster recovery and business continuity planning. We further recommend that DMR work in conjunction with WDC administrators to disseminate the comprehensive IT-related policies and procedures to all appropriate personnel once they have been formally approved and finalized. Once the IT policies and procedures have been implemented, DMR in conjunction with WDC management should develop monitoring and assurance mechanisms to ensure compliance with the established guidelines.

Auditee's Response:

> *DMR issued a policies and procedures manual entitled "DMR Security Standards and Procedures" in November of 2006. A copy of the manual has been provided to each Regional Director, Regional Operations Manager, Fiscal Manager, and Facility Director. The manual provides explicit direction regarding the physical security and environmental protection DMR expects to be exerted over IT resources by its own employees and its service organizations. The EOHHS on-site IT support person will work with EOHHS management to develop and implement operational procedures to manage the day-to-day IT operation at WDC.*

Auditor's Reply:

Documented controls, policies, and procedures provide a framework to guide and direct staff in the discharge of their responsibilities. The nature and extent of the documented IT control procedures need to address all IT functions; accommodate staff experience, competency and knowledge; and take into account any changes to IT processes, IT infrastructure, and regulatory requirements. The development of documented policies and procedures, in conjunction with DMR and EOHHS, for WDC's IT environment are necessary to help ensure that internal control practices are in effect to provide reasonable assurance that operational and control objectives will be met at the facility.

2. Inventory Control Over Computer Equipment

Our audit disclosed that inventory control practices over computer equipment needed to be strengthened to ensure that computer equipment located at WDC would be properly accounted for in DMR's system of record for property and equipment. We determined that adequate controls were not in effect to ensure that DMR management was maintaining a current, accurate, and complete perpetual inventory record of computer equipment for the Center. We found that controls needed to be strengthened to provide prompt notification and update of the inventory record when equipment is relocated, disposed of, lost, or stolen. In addition, there was no evidence that the inventory system of record had been adequately reviewed for accuracy and completeness, and an appropriate level of reconciliation was being performed. As a result, the integrity of the inventory system of record for

computer equipment could not be adequately assured. The absence of a sufficiently reliable inventory of computer equipment hinders DMR's ability to properly account for IT resources, evaluate the allocation of equipment, and identify missing equipment. We found no evidence that records of surplused computer-related items were being reconciled to ensure the integrity of the inventory records.

At the initiation of our audit, neither WDC nor DMR management could provide an inventory record for computer equipment located at the Center. We found that during the course of our audit an inventory list for computer equipment, dated August 16, 2006, was developed by DMR's site manager at WDC. Subsequently, DMR management developed what it considers to be the master inventory system of record dated, December 14, 2006. We compared both inventory records and determined that the master record did not account for 49 hardware items at the WDC. Our examination revealed that some items were microcomputers used by WDC for training, while some other items had been cannibalized for spare parts. Our audit test of selected IT assets from both lists revealed that all items were located and properly tagged. However, we found that neither list contained certain important accounting and configuration management attributes, such as acquisition dates, historical costs, installation dates and condition of the equipment. The DMR needs to ensure that appropriate controls are in place for data entry and improve its monitoring and validating of information contained in the system of record to ensure the accuracy and completeness of the information contained in the inventory system of record.

Without formal, documented, and tested procedures for performing an annual physical inventory count and reconciliation of the inventory record to purchase or lease documentation and surplus equipment records, WDC management cannot be adequately assured that their computer equipment is properly accounted for and that the inventory record is comprehensive, timely, and accurate. In addition, a periodic comparison of the computer equipment and the recorded accountability of the computer equipment will reduce the risk of unauthorized use, loss or theft of computer equipment. We believe that the weaknesses in inventory control were the result of lack of adequate monitoring and management oversight, and proper assignment of inventory control responsibilities.

Generally accepted industry standards and sound management practices advocate that adequate controls be implemented to account for and safeguard property and equipment. In addition, Chapter 647 of the Acts of l989, states, in part, that ". .. the agency shall be responsible for maintaining accountability for the custody and use of resources and assign qualified individuals for that purpose, and periodic comparison should be made between the resources and the recorded accountability of the resources to reduce the risk of unauthorized use or loss and protect against waste and wrongful acts." Sound management practices and generally accepted industry standards for IT installations advocate that a perpetual inventory record be maintained for all computer equipment and that sufficient policies and procedures be in effect to ensure the integrity of the inventory record.

Recommendation:

The WDC should establish and maintain a comprehensive list of computer equipment in conjunction with DMR. The list should be maintained on a perpetual basis, and any changes to the list should be reported to DMR and reconciled to the master system of record. Specifically, we recommend that the DMR in conjunction with WDC adhere to the control framework outlined in the Office of the State Comptroller's MMARS Fixed Asset Subsystem Policy Manual and User Guide, and its associated internal control documentation, and the Operational Services Division's guidelines regarding the accounting for and disposal of property and equipment. We recommend control procedures be implemented to ensure that the inventory records are maintained in an accurate, complete, and timely manner. The Center's inventory records should reflect any changes to computer hardware items, including location or status, for both deployed equipment and items held in storage.

We further recommend that DMR's system of record for IT inventory be expanded to include data fields containing information relative to cost, condition, acquisition installation date, and status of the IT resource. The recommended control procedures should provide increased assurance that all IT-related equipment is properly recorded and accounted for and enable the development of a complete record, maintained on a perpetual basis, of all IT-related equipment at the WDC.

Auditee's Response:

> *IT Operational services at WDC are provided by EOHHS. The EOHHS on-site IT support person has established and will maintain an inventory of all IT equipment assigned to WDC. The IT support person will be the only individual authorized to place, relocate, or remove the equipment. DMR will request that EOHHS include in their inventory application all of the inventory fields recommended by the auditors. Specifically, those fields are: cost, condition, acquisition installation date, and status of the IT resource.*

Auditor's Reply:

We are pleased that WDC is working in conjunction with DMR and EOHHS to improve inventory controls. We believe a single comprehensive inventory control system for all IT-related assets located throughout DMR facilities is an important component for the overall internal control structure. Strengthening inventory control procedures will improve the integrity of the system of record regarding computer equipment and assist the WDC, DMR and EOHHS in making IT infrastructure and configuration management decisions. We believe that controls to ensure adequate accounting of computer equipment will be strengthened by adding the additional fields of information and by perpetually updating the inventory record when changes in status or location occur and then routinely reconciling the physical inventory to the system of record.

3. Physical Security Controls

Our audit revealed that although DMR security personnel were providing adequate security throughout the facility, controls over keys to areas housing computer equipment and resident units needed to be strengthened. At the time of our audit, control over the management of keys at the Wrentham Development Center needed to be strengthened.

We found that adequate security controls were in place over areas housing computer equipment in the administrative building and file server room. We found the file server room to be equipped with a touch pad lock and protected by an intrusion alarm. We found the administrative offices to have door locks and the building had an intrusion alarm. In addition DMR security provides 24-hour patrols throughout the facility.

We found that each direct care employee at the time of their employment was given a key for all patient units for safety reasons in cases of emergency. However, our audit revealed that management did not maintain a list of authorized individuals who had been given keys and did not require individuals to return the keys once the employee terminated employment. As a result, management could not account for every key distributed and was unable to establish that only authorized employees could gain access to patient resident units. We believe that, as a result of inadequate controls over the management of the keys to client living areas, safety could be compromised and IT equipment may not be properly safeguarded. Further, the security of confidential medical and personal information residing on microcomputer workstations located in those units could be compromised.

Generally accepted security practices require that adequate preventive physical access security controls be in effect to ensure that only authorized access can be obtained. Appropriate physical security protection policies also serve to protect employees and patients from undue harm.

Recommendation:

We recommend that WDC perform a thorough risk analysis of having keys not returned or accounted for by individuals no longer employed at the Center. We recommend that WDC management immediately update its policies and procedures regarding physical security protection and in particular establish mechanisms over the control and care of keys to client living areas. We also recommend that WDC management consider either re-keying existing locks or installing touch pad locks to replace the current locks to designated secure areas and initiate a formal process for key management.

Auditee's Response:

> *Wrentham Developmental Center shares the concern of the auditors about the lack of control over the issuance and return of keys. To address this issue, the Facility Director established a formal Policy and Procedure for the distribution and collection of keys at WDC. The policy requires that all keys issued to each employee are appropriate to their level of access and that the employee sign for the keys they are issued and that they will turn in the keys upon termination of employment at WDC.*

Auditor's Reply:

We are pleased that WDC will develop and implement enhanced physical security policies and procedures over IT resources and establish a formal process for key distribution and collection. Since some areas house clients as well as hardcopy files and computer equipment, a facility management team should assess various potential risk factors in tandem with improvements in physical security and environmental controls.

4. System Access Security

Our audit revealed that system access security controls over WDC's mission-critical application systems, the Home and Community Services Information System (HCSIS), and the MediTech application needed to be strengthened to ensure that only authorized users have access to these systems. We found that although DMR had established written policies and procedures in place for the removal of access privileges for terminated employees, these procedures were not always being followed. We found that the process to inform the MIS Department at the Department of Mental Retardation when an employee terminates employment was not being applied on a consistent basis. Our audit revealed that management staff were not always providing written notification of changes in employee status, such as terminations and leaves of absences to the DMR Southeast Region's Human Resource Department. The DMR policy pertaining to access security states that:

> "*…Upon notification that a staff person has terminated employment or has been transferred to another cost center within DMR or to another state agency, the PMIS department will complete the appropriate electronic form and forward it to Central Office. Central Office staff will close all the pertinent accounts and transfer the effected individual's electronic files to a location on the network where they can be accessed by their (former) WDC supervisor. The supervisor will then review the transferred files and enact their proper disposition.*"

Our tests of access security for the HCSIS and the MediTech application systems indicated that there were active user IDs and passwords for individuals who were no longer employed by or contracted by the WDC. Our tests of the HCSIS application system indicated that 26 out 409 users were not listed on the August 7, 2006 payroll. Our audit disclosed that one of the users, who still had active user privileges, had

left the employment of the WDC in July 2004. Our audit tests of the MediTech application system indicated that four out of 313 users were not listed on the December 15, 2006 [1] payroll record.

Access to computer systems, program applications, and data files should be authorized on a need-to-know and need-to-perform basis. To ensure that only authorized access privileges are maintained, timely notification should be made to the security administrator of any changes in user status that would impact their level of authorization. For example, Human Resources should notify the security administrator of changes in employment status so that access privileges may be deactivated in a timely manner for individuals no longer needing access. Our review indicated that procedures were not always followed to inform the DMR's Human Resources Department of changes in employment status as required by DMR policy. As a result, critical information on the WDC's systems may have been vulnerable to unauthorized access, alterations, and deletions.

Computer industry standards advocate that policies and procedures for system access be in place and in effect to provide security of information assets. Management should have a control process in place to review and confirm access rights periodically. Periodic comparison of resources with recorded accountability should be made to help reduce the risk of errors, fraud, misuse or unauthorized alteration

The formal policies and procedures for system access security should be monitored so that deactivation of access privileges for terminated employees or contractors is done on a timely basis. The failure to follow written system access security policies and procedures on a consistent basis places mission critical and confidential information at risk of unauthorized access, modification, and/or loss.

Recommendation:

We recommend that the WDC, in conjunction with the DMR, perform an immediate review of the status of all active users of both the HCSIS and MediTech applications and remove all access privileges for those individuals who no longer require access. We recommend that WDC management develop written policies and procedures requiring department heads, supervisors, and the Human Resources Department to notify the regional security administrator for the Department of Mental Retardation of changes in employee status that could warrant deactivation of user accounts. We also recommend more vigilant monitoring of access accounts for WDC employees to provide additional information security controls over mission critical applications.

Auditee's Response:

Wrentham Developmental Center has reviewed the status of all users of the HCSIS and Meditech applications and has notified the DMR Help Desk to remove those individuals who should no longer have access. WDC will develop written policies and procedures that will require department heads and supervisors to notify

Human Resources when an employee's status changes necessitating the removal of access to the WDC network. EOHHS on site IT support staff, upon request will generate a list of current account holders that WDC management will verify and take corrective action as needed.

Auditor's Reply:

We are pleased that WDC will take steps to improve controls for system access security, including the action taken to remove employees who are no longer affiliated with the facility. Formalizing the communication process between department heads and Human Resources of changes in employee status and the training of supervisors in proper exit procedures for employees will enhance system access security controls. Once WDC, in conjunction with EOHHS have formally documented access security policies and procedures, we suggest that WDC periodically review them to continually meet the needs of changing IT environments and risk management objectives.

5. Business Continuity Planning

At the time of our audit, the Wrentham Developmental Center, in conjunction with the Department of Mental Retardation, had not developed a comprehensive business continuity plan, including user area plans, to provide reasonable assurance that business functions supported by technology could be regained effectively and in a timely manner. Although the DMR has procedures to back up mission critical applications for computer operations at the WDC, a formal tested business continuity strategy had not been developed. We found that there was no formal agreement in place with another organization for alternate-site processing should the LAN be unusable or inaccessible. Specific arrangements need to be made to provide for an alternate processing site. Further, WDC 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.

A business continuity plan should document the WDC's recovery strategies with respect to various disaster scenarios. Without adequate disaster recovery and contingency planning, including required user-area plans, WDC 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 at the facility. Furthermore, the absence of a comprehensive and tested disaster recovery plan could result in unnecessary costs and significant processing delays. The lack of a detailed, tested plan to address the resumption of processing by the LAN and microcomputer systems might also render data files and software vulnerable should a disaster occur.

The objective of business continuity planning is to help ensure timely recovery of mission-critical functions should a disaster cause significant disruption to computer operations. Business continuity

planning for information services is part of business continuity planning for the entire organization. Generally accepted business practices and industry standards for computer operations support the need for the WDC in conjunction with DMR to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans. To that end, WDC in conjunction with DMR should assess the extent to which it is dependent upon the continued availability of information systems for all required processing or operational needs and develop its recovery plans based on the critical aspects of its information systems.

Recommendation:

We recommend that WDC management in conjunction with DMR establish a framework of procedures to ensure that the criticality of all automated systems is evaluated and that business continuity planning is assessed for all computer operations and systems at WDC. We recommend that senior management review the information technology environment and perform a criticality assessment and risk analysis of all automated systems used by WDC. Based on the results of the assessment, DMR should proceed with the development of a written business continuity plan for WDC's mission-critical and essential functions.

Once the plan has been developed, it should be tested, then periodically reviewed and updated for any changing conditions. The DMR in conjunction with WDC management should specify the level of assigned responsibilities for maintaining the plan and for supervising the implementation of the tasks documented in the plan. Further the plan should specify who should be trained in the implementation and execution of the plans under all emergency conditions and who should perform required task to fully implement the plans. Copies of the completed business continuity and user area plans should be distributed to all appropriate staff members and kept in a secure, off-site location.

Auditee's Response:

> *WDC management in conjunction with DMR will identify mission-critical computer operations and systems and develop a Business Continuity Plan that addresses how the facility will carry on the essential functions. The plan will identify the staff to be trained and designate who will perform the required task to fully implement the plans. Once the plan is established, the plan will be distributed to all appropriate staff and kept in a secure, off-site location. The completed plan will be tested. The plan will be reviewed on an on-going basis and updated as needed.*

Auditor's Reply:

We are pleased that WDC management, in conjunction with DMR, will perform the appropriate criticality assessments and develop a business continuity plan. The business continuity strategy should be

sufficiently comprehensive to address various disaster and recovery scenarios and ensure system availability to mission-critical operations and IT processing at the facility.

Page: 15
[NMD1]Page 7 indicates the four out of 313 users were not listed on the December 15, 2006 payroll record.
Per Frank it should be December 15