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. 2004-0301-4T

OFFICE OF THE STATE AUDITOR'S REPORT
ON INFORMATION TECHNOLOGY AND FINANCIAL-RELATED CONTROLS
AT THE MASSACHUSETTS HOSPITAL SCHOOL

July 1, 2000 through October 22, 2004

OFFICIAL AUDIT REPORT
DECEMBER 21, 2004

TABLE OF CONTENTS

	Page
INTRODUCTION	1
AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY	3
AUDIT CONCLUSION	6
AUDIT RESULTS	9
1. System Access Security	9
2. Collections of Accounts Receivable	11

INTRODUCTION

The Massachusetts Hospital School (MHS), which was established through Section 446 of the Acts of 1904 of the Massachusetts General Laws as amended, provides for the care and treatment of disabled children and young adults through their twenty-first year. The statutory authority establishing MHS remained essentially unchanged until 1954 when the Massachusetts Hospital School was transferred from the Department of Public Welfare to the Department of Public Health. The hospital, which is located on 160 acres in Canton, Massachusetts, is the first facility of its kind in the United States to combine medical services and educational instruction for disabled students. The campus facilities include a hospital, elementary school, high school, and several housing units where students live during the week.

A five-member board of trustees governs the hospital. The Massachusetts Department of Public Health (DPH) and the Massachusetts Department of Education (DOE) jointly provide services at the MHS. While DPH provides administrative oversight and major funding for the hospital and non-educational resources of the facility, DOE provides additional funding and management for the education of the students. At the time of our audit, the MHS was staffed by approximately 210 employees. The hospital is fully accredited by the Joint Commission on Accreditation of Hospitals. The MHS received $13,369,694 of state funds for fiscal year 2003 and $13,295,012 for fiscal year 2004.

The MHS receives additional oversight in the form of technical support for information technology from the Commonwealth's Bureau of Hospital Management. The MHS computer operations are supported through the use of a Local Area Network (LAN) and through the Commonwealth's Wide Area Network (WAN). The LAN, consisting of three file servers and 232 microcomputer workstations, is used to process a variety of administrative and medical information. The MHS' primary application system is a vendor-supplied, integrated application known as MediTech. This application consists of seven modules: patient care, therapeutic information, medical records information, coding diagnosis, billing and accounts receivable, admissions, and electronic medical records. The MHS began its implementation of the MediTech application in August 2003 replacing the AIMS billing system. Since the MediTech application contains medical record information on individual patients, the system is subject to the security and control requirements of the Health Insurance Portability and Accountability Act (HIPAA). In addition, the MHS utilizes Windows-based applications for its fixed-asset inventory and various administrative applications.

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

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

From March 23, 2004 through October 22, 2004, we performed an audit of selected information technology (IT) and financial-related controls at the Massachusetts Hospital School (MHS) for the period covering July 1, 2000 through October 22, 2004.

The scope of our audit scope included an evaluation of IT-related controls pertaining to organization and management, physical security, environmental protection, system access security, inventory control over IT-related assets, disaster recovery and business continuity planning, and on-site and off-site storage of backup copies of magnetic media. In addition, we examined controls over the security and disposal of hard copy confidential medical records. Our audit scope also included an examination of financial-related controls pertaining to patient billing and account receivables.

Audit Objectives

Our primary objective was to determine whether adequate controls were in place and in effect for selected functions in the IT processing environment. We sought to determine whether the MHS' IT-related internal control framework, including policies, procedures, practices, and organizational structure, provided reasonable assurance that IT-related control objectives would be achieved to support business functions. We sought to determine whether adequate physical security and environmental protection controls were in place and in effect to prevent unauthorized access, damage to, or loss of IT-related assets. Our objective regarding system access security was to determine whether adequate controls were in place to ensure that only authorized personnel had access into the MHS' automated systems. Further, we sought to determine whether MHS management was actively monitoring user account management.

We sought to determine whether adequate controls were in place and in effect to provide reasonable assurance that IT-related assets were properly recorded and accounted for and were safeguarded against unauthorized use, theft, or damage. In addition, we sought to determine whether adequate procedures were in place for on-site and off-site storage of backup media to support system and data recovery operations. Further, we determined whether an effective business continuity plan was in place that would provide reasonable assurance that mission-critical IT-related operations could be regained within an acceptable period of time should a disaster render the computerized functions inoperable or inaccessible. A further objective was to

determine whether adequate controls were in place to provide reasonable assurance that hardcopy confidential medical records were subject to proper security.

Regarding our examination of financial-related activities, our primary audit objective was to determine whether adequate controls were in place to ensure that MHS was maximizing its potential revenue for patient services through proper recording, billing and collection procedures.

Audit Methodology

To determine audit scope and objectives, we conducted pre-audit work that included obtaining and recording an understanding of relevant IT operations, reviewing and evaluating certain IT-related internal controls, and interviewing senior management at both the MHS and the Bureau of Hospital Management. In conjunction with our review of the internal control environment, we determined whether MHS 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; obtained, reviewed and analyzed existing IT-related policies, standards, and procedures; and reviewed the hospital's IT strategic plan. To determine whether MHS' IT-related job descriptions and job specifications were up-to-date and reflected current responsibilities and technical knowledge requirements, we reviewed IT-related job descriptions and job specifications and compared them to current IT-related assignments and responsibilities.

To evaluate physical security, we interviewed management, conducted walk-throughs, and reviewed procedures to document and address security violations and/or incidents. Through observation, we determined the adequacy of physical security controls over areas housing IT equipment. We examined the existence of controls such as office door locks, remote cameras, and intrusion alarms. We determined whether individuals identified as being authorized to access areas housing computer equipment were current MHS employees and that access to these areas was restricted to only authorized personnel.

To determine the adequacy of environmental controls, we conducted walk-throughs and evaluated controls in selected areas to assess the sufficiency of documented control-related policies and practices. We examined the file server room and office areas housing selected IT equipment to determine whether IT resources were subject to adequate environmental protection. Our examination included a review of 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, observation, and review of relevant documentation.

We reviewed inventory control policies and procedures for IT-equipment and software by determining whether adequate controls were in place and in effect to properly safeguard and account for IT resources. We examined policies and procedures regarding fixed-asset inventory to determine whether the MHS was in compliance with the Office of the State Comptroller's regulations regarding fixed-asset control. We conducted an inventory test applying ACL audit software, which selected for review 73 out of 515 (14%) IT-related items listed on the MHS inventory, dated August 1, 2004. Furthermore, we examined the inventory record for identification tag numbers, locations, descriptions, and historical costs.

To assess the adequacy of business continuity planning, we determined whether any formal planning had been performed to resume computer operations should the network application systems be inoperable or inaccessible. In addition, we determined whether the criticality of application systems had been assessed, and whether risks and exposures to computer operations had been evaluated. In addition, to evaluate the adequacy of controls to protect data files through the generation and on-site and off-site storage of backup copies of magnetic media and hardcopy files, we interviewed MHS staff, reviewed logs and determined that the backup tapes were being rotated from on-site to off-site storage on a regular basis.

To determine whether adequate controls were in place to safeguard and dispose of confidential patient records, we examined relevant policies and procedures, conducted interviews with MHS employees responsible for patient records, and observed the areas housing confidential medical records.

To obtain an understanding of MHS billing procedures, we conducted interviews with the Acting Chief Financial Officer and staff from the Accounting Department. To assess potential risk factors regarding the recording and billing of services rendered, we reviewed the billing process and reviewed controls regarding billing procedures. Furthermore, we reviewed monthly postings to the balance sheet to determine whether collections were being recorded in a timely manner.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and generally accepted industry practices. Audit criteria used in the audit included management policies and procedures; control guidelines outlined in Control Objectives for Information and Related Technology (CobiT) issued by the Information Systems Audit and Control Association, July 2000; Office of the State Comptroller's policy manual; and state regulations.

AUDIT CONCLUSION

Based on our audit at the Massachusetts Hospital School, we determined that internal controls in place provided reasonable assurance that IT-related control objectives pertaining to organization and management, physical security, environmental protection, IT inventory control, on-site and off-site backup of computer media, and business continuity planning would be met. However, our examination of controls over system access security revealed that policies and procedures should be strengthened to ensure that only authorized personnel have access to MHS systems. In addition, we found that controls pertaining to claims that had been initially denied, needed to be strengthened to provide reasonable assurance that revenue collection is maximized for services provided at the hospital.

Our examination of organization and management controls revealed that there was an established chain of command, adequate level of oversight, segregation of duties and clear points of accountability regarding IT functions. We found that IT management and staff were well aware of their responsibilities, and that IT-related job descriptions and job specifications reflected current responsibilities, and required technical knowledge and skills. Our review of IT-related planning found that the MHS, in conjunction with Bureau of Hospital Management, had developed a IT strategic plan and policies and procedures.

Our audit revealed that physical security controls provided reasonable assurance that MHS' IT resources would be protected against unauthorized access. We found that employees were required to wear hospital-issued access cards to gain entry to the office areas. In addition, non-employees were required to wear temporary badges and were escorted during their visit. We found that the file server room was locked and that access was limited to IT personnel.

Our examination of environmental protection over the office areas and file server room concluded that the MHS had policies, procedures and appropriate control mechanisms in place to provide reasonable assurance that IT resources were operating in a controlled environment. Specifically, we found that control objectives related to general housekeeping; air conditioning; fire prevention and detection; emergency power and lighting; and emergency shut down would be met. We observed the file server room was well planned and organized and had strong environmental controls to protect personnel and equipment. The areas housing IT resources were found to be clean and environmentally protected. Although we observed that MHS had hand-held fire suppression devices, the administration building housing the file server room lacked an automatic suppression system.

Our audit indicated that access security administration needed to be strengthened for the MHS application system that supports administrative and medical operations at MHS. We found that appropriate policies and procedures were documented, security administration had been assigned, appropriate rules for user access activation and password length and composition were in place, and security requirements had been established. We found that employees were required to change passwords on a pre-defined time period. However, our tests of authorized users of the MediTech system revealed that 14 (3.3%) out of 412 users could not be identified on the MHS' May 2004 payroll record, the MHS current consultant list, or the Department of Education's list of authorized employees at MHS. Our review indicated that termination dates for the active user accounts of individuals no longer employed at the MHS, went back to early 1996. We recommend that the MHS enforce its current policy requiring that department heads, supervisors, and the Human Resources Department notify the security administrator of changes in employee status that could warrant deactivation of user accounts.

With respect to IT-related fixed-asset inventory control, we found that the MHS had developed written policies and procedures to safeguard and to properly account for all IT resources, and that the computer equipment was locatable, properly accounted for and tagged. We found that the inventory record reflected appropriate data fields including historical costs for IT resources. In addition, we found that MHS was adhering to the regulations promulgated by Office of the State Comptroller's requiring that annual physical inventories be performed.

We determined that business continuity policies and procedures were being followed regarding the generation and the on-site and off-site storage of backup copies of magnetic media. We found that the MHS, in conjunction with the Bureau of Hospital Management, had developed a business continuity strategy and recovery plans to provide reasonable assurance that IT processing could be regained within an acceptable time frame should processing capabilities be rendered inoperable or inaccessible. We recommend that MHS management periodically test all elements of the business continuity plan under its immediate control and update the plan to reflect any changes in technology, associated risks, or business requirements.

Our examination of the security and disposal of confidential records indicated that the MHS had established policies and procedures to ensure that all medical records would be safeguarded. We examined the areas in which the records were being stored and found the areas to be secure and that access was limited authorized personnel. Since the inception of the hospital, the policy in place has been to retain all hardcopy medical records therefore, none has been disposed of to date. We recommend that MHS management consider using available technology, such as digital scanning to provide more security and protection for these records.

Our review of financial-related areas revealed that controls over billing and receivables needed to be strengthened. Our review revealed that adequate controls were in place over the monthly billings and receivables except for the re-submission of Medicaid claims initially-denied Due to a reduction in staff to review, amend and re-submit initially denied claims, MHS had a revenue delinquency from July 1, 2000 through December 31, 2003 totaling $1,215,534. However, MHS management has stated that a reorganization of the Billing Department involving the University of Massachusetts Revenue Operations will provide the needed resources to reduce the outstanding uncollected revenue.

AUDIT RESULTS

1. System Access Security

Our examination of system access security for the MHS application system that supports administrative and medical operations indicated that access security administration needed to be strengthened. We found that appropriate policies and procedures were documented, security administration had been assigned, appropriate rules for user access activation and password length and composition were in place, and security requirements had been established. We also found that employees were required to change passwords on pre-defined time period. However, we found that although there were written policies and procedures in place requiring that the Information Technology Department be informed when an employee terminates employment at the hospital, there when instances where written notification was not being provided by the MHS' Human Resources Department.

Our tests of access security for the MHS application system indicated that, contrary to sound access security practices, there were active user IDs and passwords for individuals who were no longer employed by the hospital. Our tests indicated that 14 (3.3%) out of 412 users were not listed MHS May 2004 payroll, the current consultant list, or the Department of Education list of authorized employees at MHS. Our audit disclosed that one of the users who still had active user privileges had left the employment of MHS as far back as February 11, 1996. MHS policy number HR-006, dated May 2003, requires "notification by the Human Resource Department to the IT Department of changes in employment status so that access privileges may be deactivated in a timely manner for individuals no longer needing access."

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, which would impact the user's 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 there was evidence of initial authorization, and that although procedures were in place to inform the security administration of changes in employment status, those procedures were not always followed. As a result, user accounts no longer needed or authorized were not always deactivated in a timely manner. Consequently, critical information on MHS' systems may have been vulnerable to unauthorized access, alteration, and deletion.

Computer industry standards advocate that policies and procedures for system access security be documented and approved to provide a basis for proper protection of information assets. The policies and procedures should address authorization for system users, activation and deactivation of user accounts, notification of changes in user status, maintenance of authentication mechanisms and procedures to be followed in the event of an unauthorized access attempt or unauthorized access.

Recommendation

We recommend that MHS adhere to its established policies and procedures regarding written notification of changes in personnel status from the Human Resources Department to the security administrator to help ensure timely deactivation of access privileges. We further recommend more vigilant monitoring be enacted regarding the deactivation of user accounts due to changes in personnel status. We recommend that the security administrator review, on a periodic or cyclical basis, with department heads authorized to access automated systems and verify that user access privileges are appropriate to their job responsibilities.

Auditee's Response:

The Employment Services Manager, working with our Information Technology Department, has reinforced existing policies and procedures to ensure that when a person leaves MHS their access to the IT system will be stopped. There were policies and procedures in place that were not followed, thus resulting in former employees having access to our system. This has now been implemented and the MHS Hospital-wide Compliance committee will conduct periodic reviews to ensure compliance.

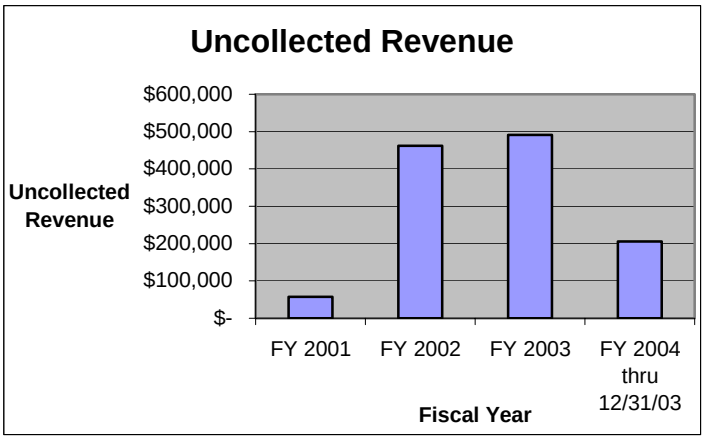
Auditor's Reply:

We are pleased that the MHS is taking steps to strengthen security to its automated systems by reinforcing the existing policies and procedures that require notification to the network security administrator of any change in employee job requirements, transfers, active/inactive status, or termination that would necessitate modification or deactivation of access privileges. We suggest that the notification procedures and subsequent modification or deactivation of user access privileges be periodically evaluated. We will examine MHS' efforts to strengthen logical access security during our follow-up audit.

2. Collections of Accounts Receivable

Our audit determined that the MHS was not maximizing its revenue collections for services provided to patients under its care. Our review disclosed that MHS was exercising proper billing control procedures for approximately $6 million in annual services billed to the federal Medicaid program. However, our review of reimbursements of claims initially rejected by the Medicaid program revealed that MHS was not researching the reasons for denial of originally submitted claim forms (UB-92) in a timely manner and, therefore, could not resubmit these claims for payment. According to MHS management the federal Medicaid program frequently denies claims due to on-going re-classification of reimbursable services. However, when a claim is researched and resubmitted by the MHS, Medicaid approves the reimbursement claim in virtually all cases**.** The failure to monitor and resubmit the claims initially denied by Medicaid resulted in MHS not collecting outstanding revenue and results in an increasing a non-tax revenue delinquency going back to fiscal year 2001. According to MHS management the cumulative delinquent amount was $1,215,534 as of December 31, 2003 in non-tax revenue due the Commonwealth. The chart below represents figures provided by MHS management.

Fiscal Year	Uncollected Revenue
FY 2001	$ 57,704
FY 2002	$ 461,681
FY 2003	$ 490,838
FY 2004 thru 12/31/03	$ 205,311
Total Uncollected Revenue	$ 1,215,534



Our review determined that MHS did not have sufficient personnel to keep the billing process current for researching and resubmitting claims originally denied by Medicaid. The Billing Department lacked adequate resources to research, adjust, and resubmit claims initially denied. The MHS relied on three permanent employees and two volunteers to perform the accounting functions for the Medicaid program. As a result of a re-organization due to a reduction in work force, the Billing Department was reduced to only two full-time employees. It is our understanding that as a result of a recent reorganization within the Department of Public Health the University of Massachusetts Revenue Operations has assumed the billing responsibility for

MHS. We believe that the corrective action being taken will result in an increase in resources to alleviate the outstanding accounts receivable as well address future claim denials in a timely manner.

Generally accepted industry standards and sound management practices indicate that adequate controls be implemented and maintained to ensure revenues are adequately collected in a timely manner and that potential revenue be maximized. In addition, the Office of the State Comptroller's regulation 815CMR 9.00 requires agencies to "make diligent efforts to collect legislatively authorized accounts receivable and debts due the Commonwealth."

Recommendation:

We recommend that MHS, in conjunction with the University of Massachusetts Revenue Operations, continue to research, adjust and resubmit all originally-denied claims from the Medicaid program to ensure that all revenues due the Commonwealth are collected. We recommend additional resources such as training be provided to staff so that claims initially denied may be corrected and resubmitted in a timely manner. We further recommend MHS management, in conjunction with the University of Massachusetts Revenue Operations, adopt comprehensive policies and procedures to monitor the timely collection of all outstanding revenue due the Commonwealth.

Auditee's Response:

> *University of Massachusetts Medical School (UMMS) Revenue Operations staff has spent the last four to five months concentrating in cleanup of the Mass Hospital School's billing module within the Meditech system. As no accounts receivables had been posted to this system, it was impossible to identify outstanding claims that had problems, from any other claims. When the MHS converted to Meditech, they brought over all balances from the prior billing system, and began billing live with Meditech as of June 2003.*
>
> *It should also be noted that when MHS began billing with MediTech there were certain charges dropping off the claims and not getting resubmitted to Medicaid due to a glitch in the system. This would not have been identified except through posting of the AR in Meditech. When UMMS; discovered the problem they had it corrected and resubmitted adjustments totaling $9,695 going back to 2003. None of these outstanding balances had been cleared within the system up to the time UMMS Revenue Operations assumed responsibility in late summer, 2004. UMMS' first area of concentration, in addition to maintaining current claim submission, was to post all remittances that related to the outstanding balances within the system. Staff has been assisting from our office in Westborough and we have concentrated primarily on Medicaid transactions.*

Once the AR posting was well underway, staff simultaneously began a second review of all remittances to locate and assess denials for rebilling potential. Hospital staff continued to process some denials for a time and many of the older remittances had notations against the denials that they had already been resubmitted. So we began with current denials and continue to work backwards. To date UMMS Revenue staff has reprocessed denials as follows and most of these were submitted within the last 2 months:

	FY2005	*$20,135 Now paid*
•	*FY2005*	*$484,345 Outstanding*
•	*FY2004*	*$ 21,165 Now paid*
•	*FY2004*	*$308,905 Outstanding*
•	*FY2003*	*$7,345 Outstanding*
•	*FY2002*	*$2,745 Outstanding*
		$844,640 *Total denials reprocessed thus far*

Work is ongoing to clear all outstanding balances either by posting of remittances or working denials. Revenue staff from UMMS' Westborough office continues to assist one or two days a week. This process is slow due to the volume and the research required going back several years in some cases. The MHS Hospital-wide Compliance committee will monitor this process to ensure compliance.

Auditor's Reply:

We are pleased that corrective action to resubmit claims originally denied by Medicaid has been initiated by MHS. We believe that the additional resources provided by the University of Massachusetts Revenue Operations will greatly assist in the researching, adjusting and re submitting of the claims to collect revenue due the Commonwealth. We are also pleased the MHS Compliance Committee has been entrusted to monitor accounts receivable collection process. We will review the efforts made to monitor and resubmit all originally-denied Medicaid claims during our follow-up audit.