Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump

Making government work better

Official Audit Report – Issued September 14, 2011

The Lemuel Shattuck Hospital
For the period July 1, 2008 through January 31, 2011

TABLE OF CONTENTS/EXECUTIVE SUMMARY

The Lemuel Shattuck Hospital (LSH), which is governed by Chapter 111, Section 69E, of the Massachusetts General Laws, is administered by the Massachusetts Department of Public Health in collaboration with the Department of Mental Health and the Department of Correction. The LSH's mission is to provide comprehensive health and support services to the community by improving the quality of life for adults who are unable to secure private health insurance. The LSH, which serves approximately 1,600 acute and chronic care patients annually, has 24 outpatient specialty clinics and a capacity of 258 inpatients.

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 LSH for the period July 1, 2008 through January 31, 2011. The scope of our audit included an evaluation of IT-related controls pertaining to physical security, environmental protection, inventory control of computer equipment, system access security, on-site storage of backup copies of magnetic media, and disaster recovery and business continuity planning. In addition, we reviewed control requirements regarding the protection of personal information as outlined in Massachusetts Executive Order No. 504 and performed a review of IT staffing levels to support information technology activities at the LSH.

We found that the LSH needed to strengthen its controls over the management of physical keys for all areas throughout the LSH facility. Specifically, our audit tests revealed that LSH management had not maintained accurate records of keys returned from former employees upon their termination and had not performed a reconciliation between a listing of individuals who had been issued keys and a listing of current employees and contractors. As a result, the LSH cannot ensure that only authorized employees have access to areas housing patients, staff, and resources or containing critical and sensitive information.

Our audit disclosed that the LSH's inventory control practices over computer equipment needed to be strengthened to ensure that IT resources would be properly accounted for in the LSH's system of record for property and equipment. Specifically, we determined that adequate controls were not in effect to provide reasonable assurance that a current, accurate, and complete perpetual inventory record of computer equipment was being maintained. 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. Furthermore, because the LSH had not performed an annual physical inventory and reconciliation as required by Office of the State Comptroller (OSC), LSH management could not be assured that the inventory system of record for computer equipment could be relied upon.

INTRODUCTION

Background

The Lemuel Shattuck Hospital (LSH), which began operations in 1954 and is governed by Chapter 111, Section 69E, of the Massachusetts General Laws, is located in the Jamaica Plain neighborhood of Boston. The LSH is administered by the Department of Public Health in collaboration with the Department of Mental Health and the Department of Correction. The LSH is staffed by 761 regular employees and 108 contract employees and is managed by a Chief Executive Officer who supervises general administrative services and directs the primary organizational divisions (e.g., clinical, nursing, professional, core services). The LSH received $72.1 million in state funds for fiscal year 2009, $69.7 million for fiscal year 2010, and $69.5 million for fiscal year 2011.

The LSH's primary mission is to provide comprehensive health and support services to the community by improving the quality of life for adults who are unable to secure private health insurance. The LSH does not offer emergency services, but does admit stabilized patients from emergency rooms, as well as patients from state prison infirmaries, county jails, and the Department of Mental Health. The LSH, which serves approximately 1,600 acute and chronic care patients per year, has 24 outpatient specialty clinics and a capacity of 258 inpatient beds.

Computer operations at the LSH consist of a local area network (LAN) supported by 10 file servers, of which nine are owned and maintained by private vendors for the LSH. The servers support 424 desktop computers, 17 laptop computers, and 134 printers. The LSH's mission-critical application, MediTech, was developed by a private vendor and implemented by the Bureau of Hospital Management. The application system supports the LSH's mission by providing automated processing information for admissions, medical records, coding diagnosis, therapeutic information, patient care billing, and accounts receivable. The application is installed on a group of file servers located at the Massachusetts Information Technology Center in Chelsea and is technically supported by Meditech Inc., which is headquartered in Canton.

The LSH's LAN connects to the Commonwealth's wide area network, allowing access to the Human Resources/Compensation Management System and Massachusetts Management Accounting and Reporting System applications that are operated at the Massachusetts Information Technology Center.

Audit Scope, Objectives, and Methodology

In accordance with Chapter 11, Section 12, of the General Laws, we performed an audit of selected information technology (IT) related controls at the LSH for the period July 1, 2008 through January 31, 2011. The scope of our audit included an evaluation of IT-related controls pertaining to physical security, environmental protection, inventory control of computer equipment, system access security, on-site storage of backup copies of magnetic media, and disaster recovery and business continuity planning. In addition, we reviewed control requirements regarding the protection of personal information as outlined in Massachusetts Executive Order No. 504 and performed a review of IT staffing levels to support information technology activities at the LSH.

We conducted this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our audit was also conducted in accordance with 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 version 4.1) issued by the Information Systems Audit and Control Association, July 2007.

The primary audit objective regarding the examination of IT-related controls was to determine whether the IT environment was sufficiently controlled to support the automated systems and provide reasonable assurance that control objectives would be achieved to support the LSH's mission. We determined 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 provide reasonable assurance that only authorized personnel had access to the automated systems. Furthermore, we determined whether the Bureau of Hospital Management was actively monitoring password administration.

We determined 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 determined whether an effective disaster recovery and business continuity plan was in place that would provide reasonable assurance that mission-critical and essential IT-related operations could be regained within an acceptable period of time should a disaster render the computerized functions inoperable or inaccessible. We also determined whether adequate procedures were in place for on-site storage of backup media to support system and data recovery operations.

Regarding the protection of personal information, we sought to determine the extent to which the LSH, in conjunction with DPH, had complied with the requirements of Executive Order 504, Order Regarding the Security and Confidentiality of Personal Information. An additional objective regarding the review of IT staffing levels was to determine the availability of staff to provide IT services to support the mission and business objectives of the LSH.

To determine the scope of the audit, we performed pre-audit work regarding LSH's overall mission and IT environment. The pre-audit work included interviews with senior management, as well as a review of documentation pertaining to policies, procedures, and internal controls. To obtain an understanding of the internal control environment, we reviewed the LSH's IT organizational structure, including interfaces with DPH and the Bureau of Hospital Management. We examined primary business functions and relevant policies and procedures, conducted formal interviews with LSH staff and management, and performed a risk analysis to identify areas of potential fraud and abuse.

Based on our review we have concluded that, during the period July 1, 2008 through January 31, 2011, LSH maintained adequate IT-related controls pertaining to physical security, environmental protection, inventory control of computer equipment, system access security, on-site storage of backup copies of magnetic media, and disaster recovery and business continuity planning. However, as noted in the Audit Results section of this report, we found that LSH's controls over physical security and inventory controls over computer equipment needed to be enhanced.

AUDIT RESULTS

1. IMPROVEMENTS NEEDED IN PHYSICAL SECURITY CONTROLS

Our audit indicated that management controls over the Lemuel Shattuck Hospital's (LSH) physical keys needed to be strengthened to ensure that only authorized individuals have keys to areas within the LSH and that areas containing critical and sensitive information are properly protected from unauthorized access. Our examination revealed that during our audit period 868 keys were distributed to individuals, including employees, medical interns and residents, and contractors who require access to areas throughout the LSH facility, including administrative office areas containing confidential medical records, patient areas, and supply areas containing medical equipment. Our audit revealed that, contrary to the LSH's security policies and procedures, logs were not being maintained for the return of access keys for those individuals who terminated employment at the LSH. As a result, LSH management cannot ensure that only authorized individuals have access to sensitive and critical areas throughout the LSH[1].

The LSH's Policy No. I.39, issued in December 2008, states, in part:

> *The Facilities Management Department will maintain the control over and responsibility for all aspects of the Lemuel Shattuck Hospital key management system. This will include the administration, tracking, distribution, cutting of keys and maintaining the lock systems.*

The policy includes detailed information regarding the procedures for the return of keys once an individual terminates employment. Specifically, the return policy outlines the following procedures:

- *Upon termination of employment, the employee will be issued Form ES-54 by the Human Resources Department and informed of the procedure for returning the key(s) to the Facilities Management Department.*

- *Once the key(s) have been returned, the Facilities Management Department will sign off on Form ES-54.*

- *The employee will return the form to the Human Resources Department.*

- *The key inventory database will be updated.*

---

[1] It is important to note that our audit indicated that enhanced security controls were in place over the LSH's pharmacy and nursing medication cabinets. We found that controls over access to these areas were closely monitored by the presence of video surveillance and supervisory oversight. In addition, we found that access to the pharmacy was limited to six individuals and required that key code access be completed within a set timeframe to gain access to the area.

Our audit test revealed that the Facilities Management Department was not being notified of employee terminations from the Human Resources Department, and we found no evidence that the key inventory database was being monitored and updated with the changes. The lack of communication between the Human Resources Department and the Facilities Management Department has contributed to LSH's inability to reconcile the distribution of keys to those employees, medical interns and residents, and contractors who have terminated their employment.

Recommendation

The LSH should immediately reconcile the authorized key record to a listing of current employees, medical interns and residents, and contractors to ensure that only authorized individuals have access to areas throughout the LSH facility and enhance recordkeeping for the distribution and return of all keys. In addition, LSH management should attempt to retrieve keys from individuals who have left employment or consider replacing the locks to designated secure areas. LSH management should also enhance communication efforts between the Facilities Management Department and the Human Resources Department to ensure the timely return and recording of access keys. Furthermore, the LSH should enforce its existing policies and procedures for security over key management.

Auditee's Response

> The Facilities Management Department has begun an inventory of all outstanding keys in conjunction with Human Resources and Campus Registration. The inventory will be completed by April 29th and the key inventory database will be updated accordingly. As the hospital department responsible for all aspects of key management, according to LSH Policy and Procedure I.39, Facilities will also be in the best position to re-key any locks that pose security risks for any employees who did not turn in keys upon departure.

> The existing Policy and Procedure I.39 is generally effective at coordinating the key exchange when state employees depart service. The policy is harder to enforce for employees in contract (especially part-time) positions where Human Resources is not involved and the contracting department manages the termination process. To resolve this potential accountability gap, the policy is being revised to require that Department Managers be accountable for signing off on the Employee Termination Checklist and to make certain that all keys are returned to Facilities Management when employees leave.

> To further ensure that all keys are being accounted for, the Facilities Department will receive a monthly report from Human Resources and Campus Registration on the latest terminations. This information will be used to reconcile the key inventory database and seek out any keys that have not been returned to Facilities Management.

> The current policy (I.39) is not workable for interns/residents, fellows, trainees and students who are issued a key to the "on-call" and conference room by Medical Administration. Their tenure on-campus is generally short-lived, usually monthly or

quarterly, and often begins and ends when Facilities Management is not open for business. Facilities Management historically relied upon the training programs themselves to manage the key exchange between departing and incoming program participants. The process is even harder to track when it involves a daily key exchange among interns and moonlighters that are providing night and weekend coverage. To promote operational efficiency and ensure security, keyless push button locks will be installed on the "on-call" and conference rooms used by these individuals. This will eliminate the need for key transfers and resolve the issue of unreturned keys. In addition the code for the keyless locks can be easily changed for security reasons and when employees leave.

Auditor's Reply

In addition to the procedures it has outlined in its response, the LSH should continue to evaluate potential physical security risks of outstanding keys and ensure that appropriate procedures are in place to sufficiently monitor compliance with the established security requirements and standards.

2. IMPROVEMENTS NEEDED IN INVENTORY CONTROLS OVER COMPUTER EQUIPMENT

Our audit disclosed that the LSH's inventory control practices over computer equipment needed to be strengthened to ensure that IT resources would be properly accounted for in the LSH's system of record for property and equipment. Specifically, we determined that adequate controls were not in effect to provide reasonable assurance that a current, accurate, and complete perpetual inventory record of computer equipment was being maintained. 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. Furthermore, because the LSH had not performed an annual physical inventory and reconciliation as required by Office of the State Comptroller (OSC), LSH management could not be assured that the inventory system of record for computer equipment could be relied upon. The absence of a sufficiently reliable inventory of computer equipment hinders the LSH's ability to properly account for IT resources, evaluate the allocation of equipment, identify missing equipment, and meet IT configuration objectives.

The Department of Public Health (DPH) provided an inventory system of record for LSH that listed IT-related assets as of August 16, 2010. Our test of the LSH inventory system of record revealed that seven (5.5%) of 128 randomly selected items were not at the locations designated on the inventory record. We were able to locate four of the items through a query conducted by LSH management and verified that the other three items had been designated by the LSH as obsolete property but never taken off the inventory record. Furthermore, during our inventory test we found an additional 10 desktop computers that were not listed on the inventory record. Also, our

examination of the inventory system of record revealed that it lacked critical data fields such as cost, serial number, and acquisition date to properly account for IT-related computer equipment.

The OSC's Accounting and Management Policy, dated November 1, 2006, states, in part:

> *There shall be a reconciliation of the fixed asset inventory against the books and records maintained by the Department . . . . This reconciliation is to be done, at a minimum on an annual basis. This reconciliation shall be available for audit either by the department's internal auditors, the State Auditor's Office or the Commonwealth's external auditors.*

Our audit revealed that weaknesses in inventory control were the result of an inadequate assignment of asset control responsibilities, and insufficient monitoring and management oversight. 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. In addition, Chapter 647 of the Acts of 1989 states, in part:

> *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.*

Recommendation

The LSH, in conjunction with DPH, should perform an immediate reconciliation of equipment deployed at the LSH to the inventory system of record to ensure the integrity of the record. Further, an annual physical inventory and reconciliation of the inventory system should be performed as required by the Accounting and Management Policy of the OSC to ensure that the inventory system of record is maintained on a perpetual basis in an accurate and complete manner. We further recommend that LSH's system of record for IT inventory be expanded to include data fields containing information relative to cost, condition, acquisition date, and installation date of the IT resource.

Auditee's Response

> *DPH IT Operations has implemented several changes effective immediately. Our internal purchasing process (AF29) has been modified to create tighter control over equipment from the point of purchase through the point of deployment . . . .*
>
> *When equipment is received at LSH, the packing slip is now scanned back to our Central Office, along with an email verifying that it has been tagged for tracking, added to the*

database and deployed. Both the packing slip and the email verification will be added to the AF29 documentation and stored electronically.

Two additional measures will be added to our control process: 1.) DPH Hospital Inventory database has been updated to include the following new fields: Cost of Equipment, Condition of Equipment at Acquisition, Install Date of Resource, and Location of Installed Resource; and   2.) Central Office will now conduct yearly, unannounced audits of technology equipment throughout all DPH locations.

Auditor's Reply

In addition to the actions initiated by the LSH to improve its fixed-asset inventory controls, we reiterate our recommendation that the inventory system of record for computer equipment be reconciled at least annually.