

THE UNIVERSITY OF MICHIGAN

REGENTS COMMUNICATION

Item for Information

Received by the Regents
April 19, 2007

Subject: Report of University Internal Audits
February 6, 2007 – February 28, 2007

Background:

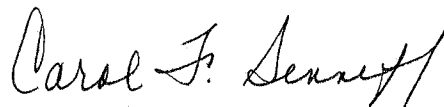
This is the report of the Office of University Audits activities for the period **February 6, 2007 through February 28, 2007**. The summaries of audits contained in this report were previously reported to members of the Regents' Finance, Audit and Investment Committee and included in discussions at Committee meetings.

Included in this report:

- Summaries of each audit report issued during the period, including Management's Plan to enhance specific control processes discussed with the audit client and presented in the report.
- Summaries of follow-up review reports issued during the period, including the actions taken by Management. Follow-up reviews are designed to give assurance that Management's Plan for corrective action has been implemented and controls are working appropriately.
- A report on the status of follow-up reviews as of **February 28, 2007**.

If you have any questions or would like additional information, please contact me at 647-7500 or by e-mail at csenneff@umich.edu.

Respectively submitted,



Carol F. Senneff, Executive Director
University Audits

April 2007

ORIGINAL REPORTS

Campus

Recreational Sports - Business Office Internal Control Review

#2007-813

Issued February 20, 2007

The objective of the audit was to determine whether internal controls adequately support business operations, safeguard assets, and promote adherence to University policies and procedures. The following processes were evaluated:

- Cash Management
- Credit Card Processing
- Timekeeping
- P-Card Utilization
- Imprest Cash Fund Management
- System Backup and Recovery

Overall, the internal control environment at Recreational Sports (REC Sports) does not provide an adequate level of assurance that assets are protected. Opportunities for improvement are detailed below. Recommendations should be applied at all REC Sports locations.

Control Issues:

- **Cash Handling** – Cash receipts are not adequately protected:
 - There is no segregation of responsibilities for receiving, reconciling, and depositing cash sales.
 - Deposits are not made within one business day as required by Standard Practice Guide section 502.1 *Department Cash Management General Policies*. During the time period reviewed, deposits were often made one to three weeks after receiving the funds.
 - There is no verification that all membership and team fees are processed appropriately.
 - The sales reports used to reconcile the main office registers are not always clear and understandable by office staff.
 - Daily equipment room and climbing wall sales are reconciled prior to placing the cash into the safe; however, there is no verification that the correct amount is actually deposited into a University account.
 - Management is reconciling the statement of activity to a report from an internal system that contains information entered by the same individual responsible for receiving, reconciling and depositing cash.
 - All professional staff has access to cash.

Management Plan – Due to limited staff, it is not feasible to completely separate the responsibilities for receiving, reconciling, and depositing cash sales. Daily reconciliations and deposits will be verified by a second individual prior to being picked up by Courier Services. The depository conversion process will be completed during March. The Treasurer's Office granted approval for Intramural Sports Building (IMSB) deposits to be made once a week for amounts less than \$500, and daily for amounts of \$500 or more. IMSB management decided to schedule regular deposits twice per week. Team fees, locker sales, and continuing memberships will be verified to source documentation on specified high-volume dates throughout the year. Data regarding the inaccuracies of the daily register reports will be collected for a month (or two if necessary) and analyzed to determine and resolve the issues.

Reconciliation of the statement of activity to source documentation will be performed by an individual who is not responsible for entering the sales into our internal financial system. These procedures will be documented. Management will evaluate which staff requires access to cash and limit it accordingly.

- Credit Card Processing – Procedures to issue credit card refunds are not compliant with the Service Level Agreement (SLA) between the Treasurer’s Office/Card Services and REC Sports.
 - Refunds are processed by the same individual responsible for sales, without review or approval.
 - Procedures do not require that credit card refunds are processed to the same credit card.
 - At the IMSB, reports that detail the entire credit card number and expiration date are not secured.

Failure to comply with the SLA may result in termination of the department as a credit card processing merchant.

There is not an adequate level of assurance that all refunds are appropriate. Credit card terminals are easily accessible with no restriction over who can issue refunds. There is no reconciliation of credit card sales and refunds per the statement of activity to the monthly reports from Fifth Third Bank.

Management Plan – Based on the environment at REC Sports, the credit card terminals will not be programmed to require a code; however, the Office Supervisors at each of the locations will review and approve all refunds before they are processed. The Office Supervisors will send the Business Manager a report of each refund with the dollar amount and associated reference number within two days of processing. The Business Manager will reconcile refunds to the Fifth Third Bank statements on a monthly basis. Hard copy credit card numbers will be adequately secured and shredded after 18 months. These procedures will be documented.

- System Backup and Recovery Procedures – The Disaster Recovery Procedures document is out-of-date and does not cover "homegrown" information systems. Also, user guides for these systems are not documented. Homegrown systems were developed for membership information and to track daily revenue by item and payment method. A current and effective plan helps ensure hardware, software, facilities and people are available to re-establish critical business systems in a timely manner in the event of a disaster. Disaster Recovery/Business Continuity plans are required by Standard Practice Guide section 601.12 *Institutional Data Resource Management*.

Management Plan – The Disaster Recovery Procedures document is scheduled for revision by the end of April, following additional upgrades to existing systems. Procedures that are not yet automated (e.g. monthly billing) have been documented and are available in an emergency. Procedures for the use and maintenance of the breakdown and membership editor systems will be documented.

- Imprest Cash Fund Management – Two imprest cash funds are not maintained at the amount consistent with Accounts Payable records. In 2005, there were two minor thefts from one fund. The thefts were reported to the UM Department of Public Safety, but the fund has never been replenished. Also, cash from one fund was used to increase the other. Standard Practice Guide section 501.2-1 *Imprest Cash Funds* requires that each fund be maintained at its original amount.

An internal cash fund is used to provide refreshments at staff meetings and appreciation lunches. The source of the fund is revenue from "left-over" t-shirt inventory and coin locker sales. Standard Practice Guide section 502.1 *Department Cash Management* states that "all funds collected by any unit or department are to be deposited into a University account on the date of collection."

Management Plan – The shortage of the two imprest cash funds will be replenished by a charge to a departmental account via Accounts Payable. The internal cash fund at IMSB from the sale of left over t-shirts and coin locker sales was deposited to a proper departmental shortcode.

- Time Report Authorization – A limited review of time reports revealed that they have not been consistently signed by a higher authority with direct knowledge of hours worked. Standard Practice Guide section 518.1 *Payroll Controls* requires that each time report be approved by the staff member's immediate supervisor or an authorized designee with direct knowledge that hours reported are true and accurate. Without proper authorization on time reports prior to entering data into the University's time administration system, employees may misrepresent actual hours worked, including adding overtime pay or not recording sick and vacation usage.

Management Plan – Time reports will be signed and approved by the appropriate supervisor who is aware of the hours worked. This change has been implemented. A document listing the authorized signers for time reports by employee will be provided to the time administrator to help ensure appropriateness.

- Inventory Tracking – The guest passes and the equipment room (ER) inventory are not adequately tracked and reconciled. Procedures exist to track guest passes checked out by the building supervisors and sold by the front door monitors; however, there is no tracking of the initial amount received or sold by the main office and no reconciliation of total sales to inventory on hand. The lack of an adequate system to track and account for all guest passes may lead to misuse of guest passes or guest pass revenue without detection. ER inventory is counted yearly and sales are tracked daily; however, without comparing the two amounts there is no assurance of proper accounting for the inventory.

Management Plan – Daily ER inventory sales sheets will be forwarded to the Business Manager, who will compare the sales to the cash register tapes. A physical count of merchandise inventory will be performed each quarter by an employee who does not work in the Equipment Rooms. This count will be reconciled to the amount of inventory ordered less inventory sold. The procedures for performing the inventory count and reconciliation will be documented. The Office Supervisor will develop and implement a plan to control all guest passes during March 2007.

- P-Card Utilization – During discussions with management, we were made aware that an employee was permitted to use her supervisor's P-Card on occasion for office supplies. P-Card Roles and Responsibilities state that only the cardholder should utilize their P-Card. While a sample review of the supervisor's P-Card statements did not reveal any purchases that appeared to be inappropriate, authorizing usage of a P-Card to someone else increases the risk for these types of charges.

Management Plan - Departmental staff has been instructed that only the P-card holder is to use his or her own card. This change has been implemented.

Auditor's Comments: During the audit, management communicated to staff the policy that no P-Cards are to be used by anyone other than the card holder. **This issue is closed.**

Overall, the control environment at the business offices within REC Sports needs improvement. Credit card processing and cash management procedures do not adequately safeguard University revenue. Improvements to imprest cash fund management, and inventory tracking will increase assurance that departmental goals are achieved and compliance with University guidelines is maintained. REC Sports was responsive in addressing timekeeping and P-Card usage concerns. University Audits will perform a follow-up review for each of the business office locations during the third and fourth quarters of fiscal year 2007 to ensure corrective actions were implemented appropriately.

Intercollegiate Athletics – Football Settlement Reports

#2007-407

Issued February 26, 2007

The Big Ten Conference requires its member institutions to prepare a “Football Ticket Sales and Financial Settlement Report” (Settlement Report) for each 2006/2007 home game. The Settlement Report shows:

- The amount of ticket revenue owed to non-Big Ten visiting teams
- The Conference share for visiting Big Ten Teams
- How the amount was calculated

NCAA Bylaw 20.9.6.3.1.1.1 requires member Division I institutions to have an annual certified audit verifying its football attendance to determine minimum average attendance of 15,000. This information is reported to the NCAA by use of NCAA Form 05-A. The Settlement Report review and the verification of football game attendance were conducted simultaneously.

The objectives of this audit were to verify the accuracy of 2006/2007 Settlement Reports and determine that information reported on NCAA Form 05-A, Attachment C, 2006 Football Paid Attendance Summary is supported by the Settlement Reports. Verification that the amount of ticket revenue was actually received and deposited into Intercollegiate Athletics accounts is beyond the scope of this audit. External auditors include revenue in their annual certified audit of Intercollegiate Athletics.

Procedures used to verify the accuracy of Settlement Reports included reviewing certified ticket stock manifests received from the printer, counting unsold tickets and verifying all computations. University Audits also reconciled each game’s attendance per the Settlement Report with the applicable NCAA Form 05-A. University Audits signed each Settlement Report attesting to its accuracy.

The amount of ticket revenue due the visiting team was accurately reported on all 2006/2007 Settlement Reports for home football games and the related NCAA Form 05-A, Football Paid Attendance Summary, was properly supported by Settlement Reports.

Information Technology

University of Michigan Health System – Electronic Signatures

#2007-305

Issued February 28, 2007

An electronic signature or e-Signature is the electronic equivalent of a handwritten signature. At the University of Michigan Hospitals and Health Centers (UMHHC), an electronic signature carries the same level of authority for the authentication of medical records as an individual's handwritten signature. The basic assumptions regarding a signature on a document, whether physical or electronic are that:

- The signature binds the signer to whatever the document states
- The document will not be changed once signed
- A signature on one document will not be transferred fraudulently to another

UMHHC uses electronic signatures in a number of applications to authenticate documents that become part of the official medical record. Electronic signatures are also used to authenticate treatment orders for providing clinical care to patients. UMHHC has created policy to control use of e-signatures. This policy requires all departments managing applications that use electronic signatures follow procedures to ensure that each electronic signature is utilized only by the authorized individual.

There are a significant number of applications at the University of Michigan that utilize electronic signatures for authentication both within the UMHHC and on campus. Based upon an assessment of risk, this audit examines certain e-signature functions within UMHHC. This audit focuses on the electronic signature function in CareWeb (used to authenticate "documents" that become part of the official medical record) and the e-signature functionality within UM-CareLink (used to validate "orders"). These e-signature processes were chosen for review because the UM-CareLink 'Signature Manager' is a model of a developing electronic signature application whereas the CareWeb 'Edit/Sign' functionality is an existing model of an electronic signature application.

Based on the audit work, controls built into the Signature Manager and Edit/Sign e-signature processes are well-designed and efficient to ensure the reliability of the e-signatures captured by these processes.

The electronic signatures that result from these processes are:

- Reliably created
- Adequately logged to ensure specific identification of signed records
- Demonstrably unique to the signer
- Adequately linked to the electronic records to which they relate

Policies, procedures, and security practices are in place to ensure trust in the electronic signatures processed by the Signature Manager and the Edit/Sign functions. Proper training processes for signers exist. **This audit is closed.**

Medical Center Information Technology Taubman Machine Room

#2007-306

Issued February 28, 2007

University Audits conducted an audit of the physical and environmental security for the Taubman Machine Room and its surrounding facility. It is one of two data centers supported by Medical Center Information Technology (MCIT) operations. Taubman is the primary computing facility for the University of Michigan Hospitals and Health Centers (UMHHC). The facility consists of four rooms and is located on the B1 level at the Taubman Health Center.

The computer room currently houses more than 400 servers containing approximately 150 terabytes (data storage measurement equal to about 153,600 billion units) of highly sensitive, extremely critical medical data.

Historically, the Taubman machine room housed large mainframe computers and was cooled by floor-mounted air conditioning units that supplied air through perforated tiles in the raised floor. As UMHHC computing demands increased and with the evolution of computer technology, the mainframes were replaced with multiple computer server units requiring more cabling under the floor. This increased cabling diminished the cooling effects and temperatures in the room escalated to unsafe levels for the machinery. In October 2001, the Regents approved a request for new ceiling-mounted air conditioning units and ductwork. Because of funding, only one unit was purchased and installed in the southwest corner of the room. This unit is unable to cool the entire 3,456 Sq. Ft. room. In 2005, an additional allocation of capital was authorized to address environmental issues in the Taubman machine room. It has subsequently been decided to discontinue any environmental upgrades to the Taubman machine room because of limitations in the electrical power that can be supplied to this site.

A new computing center has been created in Arbor Lakes Building II. With the addition of this new MCIT computing facility, the plan to address environmental and housekeeping issues in the Taubman Center machine room is to remove 40% of the servers from the Taubman Center machine room and relocate them to the Arbor Lakes facility over the next 12 months. This is designed to return the heat load of the Taubman facility to the original design thus eliminating the need for auxiliary cooling. The safety issues that go with use of fans and extension cords for power will also be mitigated. MCIT has shut down or moved more than 50 servers from the Taubman Center machine room in the last 6 months. They will be steadily removing servers over the next 10-12 months.

Physical Protection Control Issues:

- Computer Room Access – There are two sets of double doors leading into a well-traveled hallway adjacent to the Taubman computer facility. The doors from the computer room are ‘exit only’. The doors into the adjacent Tape Library are key-accessed. Unauthorized access into the computer room could be easily gained from either of the set of doors. Both set of doors are installed with outside triple-hinges which could potentially be forced open without notice. An intruder, using a screwdriver and hammer, could tap the hinge pins up and out to remove the doors for entry. These doors are not monitored at the attendant’s station nor are they alarmed to alert of unauthorized access attempts. Without monitors or alarms, either of these doors could also be propped or jammed open upon exit for reentry without notice or warning. Once inside the Tape Library, two unlocked doors lead into the computer room. All doors between adjacent rooms are within the secured Taubman Computer facility.

Management Plan – Security Services agrees there should be door position contacts on the double doors in the hallway networked to the existing UMHHC Electronic Access Control (EAC) system. The other doors leading into the machine room are within the security perimeter. Therefore, it is felt that access is already monitored. Operational controls combined with appropriate door hardware would be more cost effective for these doors. Once the Taubman machine room becomes an unmanned room, MCIT will secure the door from the Command Center into the Old Tape Library. Entry to the machine room will be made to require a keycard from the Tape Library.

- Video Surveillance – There is no video surveillance or motion detectors used inside the computer room facility. Unauthorized access and improper activity could go unnoticed especially given the number of access points to the facility.

Management Plan – The Taubman machine room is scheduled to be an unmanned facility in the near future. We will investigate the ability to monitor the Taubman Center machine room from the Arbor Lakes facility.

Environmental Support Control Issues:

- Environmental Control Plans – An environmental control plan ensures safeguarding the physical environment of the servers to increase the longevity, availability, and reliability of hardware. It addresses computer facility controls for:
 - Temperature and humidity
 - Dust or contaminants
 - Power supplies
 - Maintenance of cables
 - Security of the computer room

Environmental control plans for the machine room are included in the disaster recovery plans for the Taubman Center. However, they have not been finalized or tested. The plans are still in the process of being updated.

Management Plan – Environmental control plans were located. The systems that control the environment cannot be tested because there is no redundancy or backup AC system.

- **Insufficient Cooling** – The computer room is cooled by a central air conditioning unit that is incapable of cooling the room to an appropriate level. A large floor air conditioning unit was installed two years ago in the southwest corner of the computer room. This unit, although helpful, is unable to adequately cool the entire 3,456 Sq. Ft. room. From the location of the new air conditioning unit to the farthest side of the room, the temperature gets noticeably higher and the humidity drops lower. Eleven portable cooling units of differing sizes and types have been strategically placed throughout the room to help the cooling problem. Yet, there continues to be a cooling deficiency in the room. People and resources are at risk as long as this problem exist.

Management Plan – The plan to address the lack of cooling capacity is not to augment the existing cooling system; rather, the plan is to remove 40% of the servers in this space over the next 12 months. This will return the heat load back to the original design. Two years ago the chiller and air handling capacities were increased; however, in the time between this design and the actual increases in capacities, the number of servers increased which overloaded the ‘new’ system’s capacity. There was no longer any redundancy to allow for maintenance of the cooling system and portable coolers had to be brought in to maintain a baseline level of cooling. The portable coolers will be removed after the servers are relocated.

Hazardous Conditions Control Issues:

- **Computer Workstations** – There are several computer workstations in the Taubman computer room. The workspace for many of these workstations is extremely cluttered and potentially hazardous.

Management Plan – MCIT operations will remove all unnecessary materials from the workstations in the machine room.

- **Material Hazards** – The computer room is littered with boxes, parts, supplies, and what appear to be items left for lack of space or lack of storage. Servers, parts, and supplies are stored throughout the computer room. Cardboard boxes containing parts and supplies, plastic wrap, and other flammable materials were stacked, piled or just laying throughout the room. These boxes can be seen on the floor, between server cabinets, on server shelves, under workstation tables, behind doors, and almost anywhere a box can be placed. There were boxes, chairs, and other items that clutter the room. Dust and debris was also observed on the floor in several areas in the computer room. These conditions are hazardous to servers and persons in the computer room.

Management Plan – MCIT management will assign staff personnel to address this problem. They will remove packing materials and flammable materials that have no purpose in the room. Additionally, we will ask teams working in the room to put their supplies in the storage cabinets and to remove all spare/excess equipment. When servers are moved from the Taubman machine room to the Arbor Lakes facility and chillers are removed, MCIT will schedule a professional cleaning company to come in and clean the facility.

- **Fire Extinguishers** – Due to the presence of dust and flammable debris, high potential for fire exists in the machine room. A portable fire extinguisher is located near one of the three exits from the computer room and is behind a steel and glass panel. The single fire extinguisher is not adequate for the 3,456 square feet of encumbered computer room space. This extinguisher is not readily accessible in the event of a fire in the many potentially hazardous areas of the

room. Fire extinguishers used inside should be CO₂-based. Any "Dry-Chem" extinguishers should be replaced with CO₂.

Management Plan – As part of MCIT's commitment to a safe/secure environment, we will be documenting and posting the location of the portable fire extinguisher and reviewing the location with staff. MCIT will also order signage to further highlight the location of the fire extinguisher. As a condition of employment, every employee is required to complete a Fire Safety Learning Module and Fire Safety for Staff. We will bring this to the attention of all MCIT managers so that they may further review this finding with their staff.

Facility Services' maintenance staff performs monthly inspections of the fire extinguishers. Quantity and location of portable fire extinguishers are under the control of the Campus Fire Marshal. Two additional fire extinguishers will be added inside the Taubman machine room by Facility Operations.

- Obstructions to Exits – The computer room has many obstructions to the exits and between aisle ways. There are several blind aisles which could cause a person to become disoriented in the event of an emergency and become trapped. Over time the room has become more crowded and floor space is not being used efficiently. One door is permanently blocked by a large fan needed to help cool the room. In many cases, large fans block aisle ways causing obstructions to safely or quickly moving about the room. There were other obstructions throughout the computer room that inhibited easy movement around the room. These obstructions include small garbage pails, a ladder, several chairs, and a floor panel. Such obstructions could cause injury and prohibit orderly movement about the room in the event of a disaster. Also, none of the three exits are clearly marked for emergency.

Management Plan – UM Health Systems information technology needs grew at such a rapid rate that the Taubman machine room was forced to accommodate more equipment than its designed capacity. With the completion of the Arbor Lakes machine room facility; we anticipate removing many of the obstructions in the room. MCIT's Distributed Services and System teams are in the planning phase of moving equipment from Taubman to Arbor Lakes. As equipment is moved, we anticipate being able to remove the portable chillers, thus opening the aisles and relieving some of the power consumption.

- Electrical Cords – Electrical cords to the additional fans and cooling units in the computer room run across the floor in several areas causing a hazardous and unsafe environment for workers. Extension cords are also used for the additional cooling units. Extension cord plugs are often in the aisles and must be carefully avoided when moving about the room.

Management Plan – When 40% of the servers are removed from this space (See *Insufficient Cooling* above), there will be no need for the portable cooling units in the aisles obstructing the means of egress.

- Server Cables – Server cables are in extreme disarray. Cords are in heavy multi-colored clusters behind many of the server cabinets. These prohibit the cabinets from being enclosed to protect servers from dust and temperature extremes.

Management Plan – We concur and will take corrective action as servers are moved to the Arbor Lakes facility.

- Chiller Pipes – Two identical chillers are used in the computer room to help with the cooling problem addressed earlier. Chillers are water cooled air conditioning units. They are especially useful in rooms like basement facilities where there is no place for ductwork needed

to handle condenser air. The cooling units re-circulate water to dissipate heat using hoses which conduct the water in and out of the unit. Because of the pressure of the water passing through, the hoses must not be disturbed. The hoses on the chillers in the Taubman machine room are connected from the back of the units under floor panels. The angle of the chillers causes the hoses to be exposed. One must pay close attention to avoid disturbing the hoses as they traverse the room. One of the chillers has a hand-written sign stating, "CAUTION, HIGH WATER PRESSURE! HOSE COULD COME LOOSE". The other chiller (where the hoses are even more hazardously exposed) does not have a sign.

Management Plan – When the servers are removed from this room and relocated to Arbor Lakes, there will be no need for the portable cooling units in the aisles obstructing the means of egress.

- Computer Room Evacuation – Evacuation drills are conducted for the computer facility regularly. Drills are conducted several times a year for all shifts. However, there are no evacuation charts posted anywhere in the computer facility. This is a greater risk for the various medical staff who regularly access the computer facility to support their unit's servers.

Management Plan – An evacuation chart has been posted within the machine room. **This issue is closed.**

- Shut-down Procedures – Procedures for an orderly shutdown of the computer facility, in the event of a major disturbance, are under development. Scenario testing was conducted in 2004. However, the procedures were never completed.

Management Plan – Operations Management will perform an investigation. They will then contact MCIT teams having equipment in the machine room to discuss prioritizing the development and documentation of orderly shutdown procedures for the Taubman Center machine room.

Because solutions to a number of the issues raised are dependent on the relocation of hardware from the Taubman Center machine room, a follow-up of outstanding issues will be conducted during the second quarter of Fiscal 2008.

UMMS Surgery – Research Labs IT Security

#2006-403

Issued February 28, 2007

Surgery labs were surveyed regarding the sensitivity of data, storage locations, physical and logical access controls, encryption mechanisms, and backup/recovery processes in place. Controls reported by each individual lab were not tested. Our goal was to obtain an overview of the controls in place by:

- Identifying high-risk computing practices in research labs
- Characterizing the overall level of data security risk
- Identifying the current IT support structure for the labs
- Evaluating the IT environment's support of internal controls over data access, integrity, and availability
- Identifying opportunities for improved communication, service levels, and efficiency

The short-answer survey netted 34 responses from a population of approximately 50 labs. Survey results, controls, and labs' IT needs were discussed with:

- Business administrators in the Department of Surgery
- MCIT management supporting Surgery's administrative offices
- MCIT management and staff supporting Health System research labs, including some in Surgery

- Management in MSIS (Medical School Information Systems)

Security and control issues were identified, and should be addressed locally within the Department of Surgery and its labs. Our findings also pointed to more pervasive issues within the Health System, which are discussed separately at the end of this report.

Control Issues:

- Critical Data Stored on Workstations – Over 40% of the labs reviewed in the Department of Surgery store Electronic Protected Health Information (EPHI) or unique research data on their workstations. Such data is more appropriately stored on a network, where the risk of unauthorized access, theft, and loss is typically much lower.

The cost of procuring networked file storage space is a significant factor for labs deciding to store data locally. Surgery research labs currently receive some file space from MCIT via the Surgery Department, but it is not enough. Surgery Administration has been seeking affordable sources of additional file space that it may purchase or negotiate for on behalf of labs:

- MCIT offers supplemental file space which is designed and priced on a clinical model.
- MSIS is preparing to offer file space to Medical School departments and labs at a lower price, but it is not yet available.

Information Technology Central Services (ITCS) also offers networked file space. Their pricing compares favorably with that of MCIT and MSIS.

- Encryption of Mobile Data – Encryption of files or disks is not practiced by any of the labs reviewed, yet nearly 25% demonstrate increased risk factors that encryption could mitigate:
 - Storing Electronic Protected Health Information (EPHI) or other research data on workstations
 - Using laptops or mobile storage devices

The data encryption method arguably most convenient and effective – automatic encryption of whole disks or devices – is not currently available from any of the interviewed IT service providers supporting Surgery research labs. Such solutions are currently in testing.

- Data Backups - Over half the labs reviewed do not rely on managed file servers for primary data storage, making backup of lab workstations a key control. Of these labs, most backup data by manually writing files to CD or copying files to portable hard disks. A small portion performs no backups.

Backup planning is carried out separately in each lab. This is a flexible approach, consistent with the autonomy generally accorded research labs at the University. However, it shifts the entire burden of designing and managing effective data backup to individual labs that may lack necessary expertise. The backup plans supplied by labs were inconsistently and incompletely described as to the frequency of backup, media storage location, testing, and retention periods.

Given the broad scope of this review, a detailed evaluation of each lab's approach to data backup was impossible. However, the evidence suggests that the consistency, regularity, documentation, and testing necessary for backup processes to assure preservation of data and continuity of research activity are not present.

- Skilled Systems Administration - Over 40% of labs reviewed have systems that are not administered by an IT service provider. In many cases, administration must be performed by lab members. Systems administration arrangements are made by each individual lab. Department of Surgery business administration has not played a role.

Systems administrators are expected to perform several key controls:

- Update and patch critical software promptly
- Document standard procedures and practices for data backup, account maintenance, system monitoring, hardware/software configurations, etc.
- Limit system access to what is necessary to accomplish assigned duties, i.e., promote the concept of "least privilege" access
- Cleanse computers, storage media, and electronic devices of confidential information before disposal

Trained IT professionals are best equipped to perform these duties in a reliable, efficient, coordinated manner.

Several labs indicated difficulty procuring systems administration services. The most frequently cited obstacle was obtaining supportable computer hardware. MCIT support is optimized for Windows PCs purchased in standard configurations from Dell. Labs that cannot afford to purchase such systems cannot obtain MCIT support.

Nonetheless, over 40% of the labs reviewed indicated they are currently supported by MCIT. In the broader UMHS research environment, MCIT estimates they support roughly one-third of labs and are actively seeking to expand.

Labs that do experience difficulty getting support from MCIT have other options. Several of the labs reviewed are supported by some other IT service provider, such as ITCS Contract Services or an associated academic unit's IT staff.

SUMMARY

Some level of IT control was present in every lab reviewed in the Department of Surgery. Password access controls and physical safeguards were nearly universal, and the majority of labs' systems were professionally administered.

Nonetheless, over half these labs carry an elevated risk to the confidentiality, integrity, or availability of EPHI or unique research data. The most significant contributing factors have been discussed here:

- Storage of EPHI on workstations
- Use of laptops or mobile devices (particularly when sensitive data is not encrypted)
- Lack of professional system administration
- Absent or unreliable data backups

These substantial risk factors are not adequately controlled. We have provided recommendations that contain suggested approaches for the labs and the Surgery Department to mitigate them.

MANAGEMENT RESPONSE

The Department of Surgery understands the risks and recommendations outlined in the report. The Department believes that the recommendations fall into two distinct categories: departmentally focused solutions and central IT solutions.

The Department will request and advocate for the following central IT solutions that are beyond the Department's ability to provide:

- Increased storage space on centrally supported servers
 - Modifications from MCIT to their standard desktop computer image to facilitate the use of non-MCIT networked storage resources
- Managed encryption of mobile data files and devices

The Department has identified the following tasks that it can do internally to help moderate or eliminate the risks listed in the report:

- The Department will team with MCIT desktop services assigned to research to visit each research lab that is not currently using MCIT services and analyze the potential of switching to MCIT desktop support.
- The Department will develop a policy for IT controls within labs that cannot (for technical reasons) utilize MCIT support. This policy will provide guidance on security and backup of data, and will be drafted and communicated prior to July 1, 2007.
- This report will be shared with all sections within the Department to increase awareness of the risks.
- The Department will continue engaging the research labs and IT service providers to identify and implement solutions to data security issues.

AUDITOR'S COMMENTS

We will follow-up on the Department of Surgery's progress in implementing corrective action during the fourth quarter of fiscal year 2007.

SUMMARY – HEALTH SYSTEM

The IT security issues identified in the Department of Surgery research labs are not unique. We believe the same needs, issues, and risks could be found in many research labs in many areas of the Health System.

Survey results showed a correlation between MCIT support and overall IT risk scores which suggests that having MCIT support may improve risk posture. Given the above-average rate of MCIT support adoption by Surgery labs, it is likely that risk scores in other Health System departments' labs would be poorer.

The IT risks identified during this review are rooted in the inadequacy of basic computing services and support: working storage, backup and recovery, system security, system administration, desktop support, and hardware resources. Based on our observations and discussions with management, a number of factors contribute to this situation:

- Diverse lab needs – such as custom-developed or niche software, special hardware, and extra space – conflict with IT service provider standards
- Diverse lab funding sources produce accounting difficulties
- Unclear bounds of responsibility between the largest Health System IT service providers, MCIT and MSIS
- Sustainable funding arrangements for expanded MCIT service and support
- Desire for lab autonomy

These underlying issues require clarification, prioritization, and resolution that can only be achieved through Health System leadership.

Based on a review of current literature, the Health System could adopt two governing philosophies in addressing the underlying issues and increasing IT support for research labs:

- Increase coordination between labs, departments, and IT service providers to enable researchers to make informed decisions regarding IT systems and security
- Increase the adequacy of – and reliance on – centrally provided services at the school, center, or Health System level

Blending these two philosophies may be appropriate. Coordination would allow researchers to continue managing IT resources independently if needed, while remaining informed of the scope of responsibilities they have assumed. Coordination alone, however, is unlikely to enhance oversight and

assurance. Centrally provided services, adopted wherever possible, can be more effectively monitored, controlled, and optimized.

The benefit from undertaking such an effort would include:

- Enabling more researchers to focus on their primary mission – not IT support
- Uniformity of IT costs charged to grant sponsors
- Increased leverage of existing Health System IT investments

A program for ensuring that all Health System research labs have adequate basic IT services and resources would also reduce risk by:

- Eliminating barriers that discourage safe computing behavior
- Supporting implementation of IT security controls
- Facilitating compliance with institutional security policies
- Improving auditability

By adopting such a program, the Health System would significantly reduce the risk of losing unique research data or exposing confidential clinical data.

FOLLOW-UP REPORTS

UMHHC Vendor Discounts, Allowances, and Rebates

#2006-119

Original Report issued July 19, 2006

Follow-up Report issued February 15, 2007

Depositing – Significant progress had been made in eliminating excessive depositing delays. Vendors that send rebate checks were contacted and informed to send all checks directly to the UMHHC Contracts and Procurement Office.

The Contracts and Procurement Office usually deposit vendor rebate checks within a few days after reviewing payments, recalculating amounts for reasonableness, and determining the correct chartfields. Vendor rebate checks can be quite large and frequently exceed \$10,000. University cash management policy requires departments to make deposits within one business day of collection. **Issue remains open**

We will re-contact the Contracts and Procurement Office in May 2007 and verify that deposits are made timely.

Utilities Services Energy Billing System

#2005-337

Original Report issued November 2, 2005

Follow-up Report issued February 26, 2007

- Business Continuity Plan - Utilities Services has completed and implemented a business continuity plan which complies with University guidelines. **Closed**
- Password Controls - The vendor has included encryption of the configured password in the newest release of the Energy Billing System (EBS) client which has been scheduled for installation by Utilities Services. **Closed**
- Security Monitoring - Security policies have been completed and reviewed by University Audits. **Closed**
- Virtual Firewall - The servers hosting the Energy Billing System currently use operating system firewalls for protection of the application. The virtual firewall will be installed for this area in March. These controls are adequate to protect the data. **Closed**

Management has taken appropriate corrective action. **This audit is closed.**

- Server Security – At the time of the audit, no one was assigned responsibility to install and test updates to the operating system on the server hosting the Access Control System (ACS). University Audits recommended that Security Services assign responsibility for maintenance and monitoring of the operating system, run a security scan monthly to identify potential vulnerabilities and assign individual accounts for 'superuser' access to the operating system on the server.
Security Services made the decision to move the application to an MCIT-administered server. This ensures that operating system and virus updates are made on a timely and systematic basis. Periodic scanning has begun. The implementation of individual 'superuser' accounts has been scheduled for late spring or early summer. **Closed**
- Vendor Remote Access – At the time of the audit, Security Services used a remote vendor-supplied diagnostic service for application support. This necessitated that a modem be connected to the ACS server. University Audits recommended that Security Services determine whether remote access support was required. Security Services has changed support vendors. They determined that remote dial-up support was not necessary and the modem has been eliminated from the new server. **Closed**
- Operations Procedures and Cross-training – Written procedures required to administer the ACS application had not been prepared and cross-training for system support functions needed to be completed. Documentation of critical procedures such as client and server password controls and backups have been completed by Security Services and reviewed by University Audits. Backups within Security Services have been identified and cross-trained for the one staff member who has much of the responsibility for activities supporting the ACS application. **Closed**
- Access Control Unit and Security Procedures - Security Services was in the process of developing written policies, procedures, and guidelines specifically addressing data security for the Access Control unit. University Audits recommended that Security Services establish and communicate internal policies and procedures for use, audit, and release of ACS data.

Security Services agreed to prepare the additional written policies, procedures and guidelines for the ACS. A CCURE 800 Release of Information Policy and Procedure documenting the use, audit, and release of ACS data has been developed by Security Services and reviewed by University Audits. **Closed**

Management has taken appropriate corrective action and the control environment has been strengthened. **This audit is closed.**

- Accurate Discharge Planning Codes – All Final Plan discharge codes have been updated in CareWeb for accurate discharge disposition tracking. The UMH Coding Unit's "Smart System" edit program was updated to check that all of the 182 Diagnosis Related Group codes are consistent with the current Center for Medicare and Medicaid Services (CMS) continued care disposition codes.
- Post-Discharge Changes to Discharge Disposition Code – Discharge tracking sheets are included in home care referral packets and faxed to home care agencies for completion and

return within 48 hours. Changes to post-discharge codes are currently captured in CareWeb as a progress note. A “Practice Management Addendum to Final Plan” template has been developed and will be implemented in CareWeb when technical support priorities permit. A protocol has been established with the UMH Coding Unit for communicating post-discharge changes.

- Discharge Disposition Code Fields – Discharge disposition codes have been revised and embedded in the CareWeb Final Plan documentation. Manual review of a sample of discharge records for each practice management coordinator will be performed every six months and results will be incorporated into performance evaluations.
- Coordination between Hospital Services – Coordination between services will be rolled into the new UMHS Orders Management Project. CareWeb documentation has been revised to include a case conferences section. A CareLink referral process from the Emergency Department to Discharge Planning is currently under consideration. In the interim, referrals will be communicated through rounds, voice mail, paging, and e-mail.

Management has taken, or is in the process of taking, appropriate corrective action on major audit recommendations. **This audit is closed.**

University Audits – University of Michigan
Open Audits Follow-up Table
February 28, 2007

Audit Title	Report Date	Status	Expected Completion
UMHHC Radiology IT Security 2005-338	5/23/06	Management is addressing issues related to physical access to the server room, passwords and user IDs	March 2007
UM Medical School Anesthesiology IT Security 2006-404	9/29/06	Removal of SSNs from the Centricity system, physical access to the server room and securing workstations in public areas are the issues still being addressed	March 2007
UMHHC Pathology IT Security 2006-401	9/29/06	Installation of another proximity card reader on Pathology's server room and implementation of a periodic review of access are the outstanding issues for follow-up	March 2007
University of Michigan Computing Environment CoSign Web Authentication 2006-303	11/28/06	Issues being addressed include relocation of a server and formalization of departmental procedures	June 2007
Credit Card Processing 2006-121	11/30/06	The Treasury Office is updating the Service Level Agreement with merchants across campus	March 2007
MCIT Taubman Machine Room 2007-306	2/28/07	MCIT is addressing environmental problems in the Taubman machine room; also moving 40% of servers to new Arbor Lakes computer room	September 2007
UMMS Surgery Research Labs IT Security 2006-403	2/28/07	Department of Surgery is addressing issues related to IT administration and security	June 2007
Professional Fee Billing Compliance 2005-126	12/22/05	New organizational structure has been established. Report is being written.	March 2007
UMHS Mlabs 2006-112	1/19/06	Management has implemented corrective actions. Report is being reviewed.	March 2007
UMHHC Vendor Discounts, Allowances, and Rebates 2006-119	7/19/06	A review was conducted in February 2007. Deposits are made more often but still are not on a daily basis when large dollar amounts are received.	May 2007
UMHS Materiel Services Center 2006-106	9/29/06	Identification of staff authorized to receive goods, reconfiguration of the dock to restrict access, pre-numbering receiving reports and conducting periodic cycle counts are the open issues	March 2007

University Health Services – Charge Capture and Inventory Management 2006-111	11/14/06	Strengthening controls over billing and cash handling; formalizing related procedures	March 2007
Graduate Medical Education – Veterans Administration Billing 2006-128	11/30/06	Improving procedures that support billing from the VA for UM Graduate Medical Education	April 2007
Michigan Public Media Phase I 2006-806	3/24/06	Policies have been documented and communicated to all staff	Follow-up memo issued 7/31/06 2 nd follow-up planned for March 2007
Michigan Public Media Phase II 2006-806	4/24/06	Significant reorganization and implementation of control policies and procedures is in progress	March 2007
Library Special Collections 2006-205	6/16/06	Library administration is working to strengthen the controls discussed during the audit	March 2007
Intercollegiate Athletics Sports Camps 2006-410	7/28/06	Operational improvements are being implemented regarding background checks, contracts, financial records, reconciliations, time away policy and cash management	March 2007
College of Engineering – Minority Engineering Program Office 2006-813	9/29/06	CoE and MEPO created a thorough management plan to address the audit issues; will review progress ongoing	April 2007
Office of the VP for Research Animal Care Administrative Processes 2006-102-3	9/29/06	Management in units and centrally will address action plans	March 2007
NCAA Compliance – Recruiting 2007-405	11/16/06	Improving the quality of recruiting support documentation	June 2007
Autism & Communication Disorders Center 2006-814	11/22/06	Procedures will be documented	May 2007
Procurement Services Procurement Card Program 2007-115	2/5/07	Phase I - Procurement Services will utilize data mining tools and reduce transaction based monitoring; additional focus on training and accountability of P-Card approvers, provide guidelines for card issuance, and utilize electronic resources. Phase II – annual monitoring of card activity by dept.	Phase I – June 2007 Phase II – March 2008
Recreational Sports Business Office Internal Controls Review 2007-813	2/20/07	IM Building procedures were reviewed but action plans will be implemented in all Rec Services locations	June 2007