

THE UNIVERSITY OF MICHIGAN

REGENTS COMMUNICATION

Item for Information

Received by the Regents
September 18, 2008

Subject: Report of University Internal Audits
May and June 2008

Background:

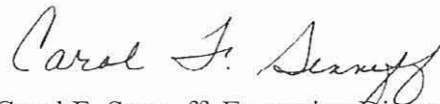
This is the report of the Office of University Audits activities for the period **May 1, 2008 through June 30, 2008**. The summaries of audits contained in this report were previously reported to members of the Regents' Finance, Audit and Investment Committee and included in discussions at Committee 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 **June 30, 2008**.

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

Respectfully submitted,



Carol F. Senneff, Executive Director
University Audits

University Audits
May and June 2008 – Summary of Reports Issued

ORIGINAL REPORTS

Campus

Office of the Vice President for Communications Fiscal Responsibilities

#2008-211

Issued May 30, 2008

University Audits conducted an audit of the Office of the Vice President for Communications (OVPC) focusing on fiscal responsibilities. The OVPC is the main communications advisory unit for the University of Michigan. The OVPC units include News Service, Public Affairs and Media Relations, Michigan Marketing and Design, Executive Communications, and the Policy and Administration and Freedom of Information Act (FOIA) Office.

The primary objective of the audit was to review central and unit processes of the OVPC. University Audits examined the following processes to evaluate the adequacy and effectiveness of internal controls over fiscal responsibilities:

- Revenue processing
- Cash and credit cards
- Expenditures
- Payroll
- Time tracking
- Budgeting
- Temporary and student employment
- Equipment and vehicles

University Audits observed that the OVPC has good documented policies and procedures. The OVPC and its units are continuously working to improve the control environment and to gain efficiencies. Photo Services, an auxiliary unit under News Service, recently completed a significant project to become compliant with the Treasurer's Office requirements regarding electronic credit card transactions. To be cost effective, Michigan Marketing and Design is working with Procurement to obtain contracts with its major printing vendors. The OVPC assets and equipment are adequately tracked and safeguarded.

Control Issues:

- Segregation of duties - University Audits identified several processes where segregation of duties could be improved. Specifically:
 - Gross pay registers are not reconciled to the original source documents by staff members independent of time entry and the reconciliation is not reviewed by a higher administrative authority.
 - The duties of invoicing external clients, collecting payments, and making deposits for the University Record are performed by the same employee.
 - Charges to University Record clients are downloaded from a FileMaker database, used to capture all advertising information, and reconciled to the newspaper issues for the billing period. The charges to internal clients are then entered manually into a spreadsheet for upload to the Service Unit Billing system. The manual billing process is inefficient and revenue transactions may be missed.

Recommendations regarding Segregation of Duties:

- An employee independent from the timekeeper should reconcile the hours reported on the gross pay registers to the original time documents. A higher authority should perform appropriate monitoring and regular review.
- University Record Management should segregate the duties of invoicing customers, and collecting payments and making cash deposits.
- University Record Management should investigate a method to create the Service Unit Billing spreadsheet directly from a download from the FileMaker database. If a download is not feasible, an independent employee should verify the accuracy and completeness of charges before processing in the Service Unit Billing system.

Management Plan:

- Management incorporated the aforementioned controls regarding gross pay registers in the Employment Process policies/procedures and communicated them to all management staff.
 - Management has identified and designated different staff members to prepare the invoices, collect payments, and make the cash deposits to ensure that proper segregation of duties is maintained.
 - Management, with the guidance of IT support staff, will determine if an automated download is feasible. As an interim measure, Management has designated a staff member to check the work of the office manager who processes the charges.
- P-Cards - Unit directors who do not have P-Cards charge some travel expenses on staff members' P-Cards. These same directors are the P-Card approvers. There is no additional P-Card statement review from a higher administrative authority.

The Vice President for Communications has delegated his authority to approve P-Card statements to the Senior Business Manager. Delegation of authority is not properly documented. The Senior Business Manager approves the P-Card statements of the Chief of Staff, her direct supervisor.

Management Plan – Management has communicated the importance of a second review of the administrative assistants' monthly P-Card statements to the unit directors. The second review eliminates any risks associated with the use of the P-Cards. This will be included as part of the OVPC policies and procedures.

The Vice President for Communications will sign the "P-Card Maintenance Forms" to document delegation of authority for P-Card statements. In addition, the Vice President and the Senior Business Manager will perform a joint review of the Chief of Staff's P-Card statements during their monthly meetings.

- Delegation of Authority - The Vice President for Communications has delegated his authority to approve P-Card statements to the Senior Business Manager. Delegation of authority is not properly documented. The Senior Business Manager approves the P-Card statements of the Chief of Staff, her direct supervisor.

Management Plan - The Vice President for Communications will sign the "P-Card Maintenance Forms" to document delegation of authority for P-Card statements. In addition, the Vice President and the Senior Business Manager will perform a joint review of the Chief of Staff's P-Card statements during their monthly meetings.

- Cash Deposits - The OVPC units make deposits of cash and checks. Deposits are not done in a timely manner. Standard Practice Guide 502.1 requires University units to make deposits on the day of collection.

When this is impractical, or the deposit is less than five-hundred dollars, the deposits should be made within one business day of the collection. Exceptions to this policy must be approved by the Treasurer's Office.

Management Plan - Management has received approval from the Treasurer's Office for Michigan Marketing and Design to make weekly deposits provided their funds do not exceed \$100, in which case the funds are to be deposited within one business day. All other units within the OVPC will follow the Standard Practice Guide. This has been communicated to all unit directors and their staff. As of the date of this report, this practice has been implemented.

- Web Yellow - Web Yellow is a database developed in-house by Michigan Marketing and Design (MM&D). The database is used to create and track projects, report hours, record and track expenses by project and vendor, generate invoices, bill clients, and process revenue in the University's Service Unit Billing system. University Audits identified the following opportunities for improvement related to Web Yellow:
 - MM&D performs regular backups of the Web Yellow server. Back-up tapes are stored in the server room and in the systems administrator's house. MM&D should contact their IT support provider and have their Web Yellow back-up tapes stored in a secure location administered by the University.
 - MM&D is continuously improving Web Yellow functionality features. The upgrade procedures and system changes are not properly documented.

Management Plan:

- MM&D Director and the IT staff took immediate action to implement daily backups via the ITCS TSM (Tivoli Storage Manager) offsite network backup system for the Web Yellow server. In addition, MM&D will perform daily backups on rotating tapes.
- MM&D Director, IT staff, and the Administrative Manager took immediate action to implement an official upgrade log for Web Yellow and communicated this to the appropriate staff.

Based on the audit work conducted, University Audits determined the overall control environment within the OVPC is sound. University Audits will conduct a follow-up review in the first quarter of fiscal year 2009 to assess progress on management action plans.

Intercollegiate Athletics NCAA Directed Review

#2008-404

Issued June 19, 2008

As a member of the National Collegiate Athletic Association (NCAA), the University of Michigan is obligated to comply with NCAA rules and regulations. University Audits performed a directed review of key NCAA compliance areas to help provide Athletics with assurance that existing procedures to monitor compliance are adequate. The Athletics Compliance Services Office (CSO) advised University Audits as to which compliance areas and specific procedures should be included in the review. University Audits did not perform a complete risk assessment of the compliance areas and the procedures performed may not address all NCAA requirements in the respective areas.

University Audits and CSO discussed that the goal will be to perform this directed review annually to include all sports over a five-year cycle. Procedures will also include a review of select external camps and booster clubs to confirm an adequate system for tracking financial activity.

Based on the specific testing performed, University Audits did not observe any issues of non-compliance with NCAA rules and regulations relative to rules education, playing and practice seasons, coaching staff limits, financial aid, eligibility, recruiting, sports camps, boosters and complimentary tickets. Overall, the external camps and booster clubs reviewed have an adequate system for tracking and maintaining financial records. University Audits will meet with the CSO during the second quarter of fiscal year 2009 to discuss the directed review procedures for the next year.

University Audits conducted a review of the University of Michigan School of Dentistry (SoD) to assess compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The Administrative Simplification provisions of HIPAA require the Department of Health and Human Services (HHS) to establish national standards for the security of electronic health care information. New technologies developed as the health care industry began to move away from paper processes and rely more on digital records. These technologies necessitated the development of security standards over critical data. Prior to HIPAA, no generally accepted set of security standards or general requirements for protecting health information existed in the health care industry.

The HIPAA Security Rule was published in the Federal Register on February 20, 2003. The final Security Rule specifies a series of administrative, technical, and physical security procedures for covered entities¹ to use to assure the security and confidentiality of electronic protected health information (EPHI)². There are both civil and criminal penalties for noncompliance with HIPAA regulations.

HHS has responsibility for ensuring compliance with the HIPAA Security Rule. In March 2007, the first covered entity was audited by the Office of the Inspector General at HHS. This review was viewed by the health care industry as a precursor to similar audits of compliance with the HIPAA Security Rule at other institutions. To assess the readiness of the SoD for a similar review of HIPAA compliance, HIPAA IT security was reviewed based upon a published list of 42 items that were requested by HHS officials during the initial HIPAA audit. In addition to those guidelines, the following EPHI issues were examined at the request of Dental Informatics management:

- Off-site/personal storage of EPHI data by graduate students and faculty
- Use of EPHI data by students and professors
- Time-out sessions on terminals when working with EPHI data

The objectives for this audit were to:

- Determine that policies and procedures exist for securing EPHI in compliance with HIPAA.
- Determine that security practices are consistent with existing policies and procedures and compliant with HIPAA requirements.
- Determine if students and faculty transfer EPHI data in a well-controlled manner onto secure mobile devices (laptops, removable hard drives, flash drives, etc.).
- Determine if students and faculty store EPHI data properly on computers (desktop and /or laptop).
- Determine if terminal session time-outs on devices and applications containing EPHI data are adequate to provide control.

Control Issues:

- Required Security Policy - The policies and procedures being developed for monitoring remote access to systems, patch management, and reviewing activity in systems containing EPHI should be completed,

¹ Under HIPAA, this is a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a HIPAA transaction.

² EPHI is Electronic Protected Health Information which is made up of items such as medical record numbers, account numbers, or SSNs. EPHI also includes patient demographic data, e.g., address, date of birth, date of death, sex, e-mail/web address, and other records such as date of admission, or discharge and treatment records such as medical records, reports, test results, appointment dates.

approved, and disseminated to appropriate School of Dentistry students, faculty, and staff. These procedures should include actions steps to address the threat of exposing sensitive information.

Management Plan - The policy and procedures for monitoring systems and the network will be finalized, approved, and disseminated to the appropriate staff.

- Personal Storage of EPHI - School of Dentistry students are required to do case presentations. They prepare these presentations by moving full facial photos of patients to their laptops; then working on the presentations at home. There is a definite need for students to have access to this data for completing required course work. However, without proper security over laptops and flash drives, this sensitive, patient-identifiable data are at risk of being compromised. Security practices and/or policies can help to ensure awareness to protect this sensitive patient data.

Management Plan - The School of Dentistry is discussing implementation of a number of controls where patient data are needed for schoolwork. Management is assessing a variety of possible solutions which include use of policies, training, devices, and software controls.

With the exception of the items listed above, controls at the School of Dentistry Dental Informatics are consistent with the HIPAA Security Rule requirements. Developing, finalizing, and disseminating policies and procedures will strengthen controls and help ensure compliance by all faculty, students, and staff.

A formal follow-up review of the School of Dentistry management actions will be conducted during the third quarter of 2009.

Healthcare

University of Michigan Hospitals and Health Centers Emergency Department
Issued May 9, 2008

#2008-112

University Audits conducted an audit of the internal control environment within Emergency Medicine of the University of Michigan Hospitals and Health Centers. The Department of Emergency Medicine is a full-service Level 1 adult and pediatric trauma center that provides emergency care 24 hours a day, 7 days a week.

University Audits examined the following processes to evaluate the adequacy and effectiveness of internal controls governing the Emergency Department (ED):

- Patient registration
- Charge capture
- Patient discharge
- Supply and drug inventory
- Patient information

Our audit focused on the Emergency Department divisions of Main Emergency Services and Children's Emergency Services. Psychiatric Emergency Services, a section of the Department of Psychiatry, was not included in this review.

Control Issues:

- Discharge Process Opportunity - The Emergency Department is not equipped with a secure check-out location. Therefore, financial services, such as collection of uncovered fees and financial counseling, are not provided during the discharge process. All medical fees, including co-pays and deductibles, are subsequently billed, and collection efforts occur considerably later than the date of service. A secure check-out location would allow the opportunity to provide financial services before the patient leaves the premises.

Management Plan - The Outpatient Revenue Cycle Advisory has initiated the Patient Pay Strategy Project, an institution-wide effort. This project focuses on several components, including increasing cash collections at point of service, technology improvements (e.g., real time eligibility/verification, charge estimates), and patient account collection efforts. Responsibility for ED cash collection has been assigned to the ED Registration team of the Business Services department. The director of Business Services is a member of the Patient Pay Strategy Project Team and is working through the steps needed to implement cash collection in the ED once the physical space is ready.

- Medical Documentation - Patient transfer forms are not consistently completed for patients transferred from the U-M Emergency Department to external facilities. ED procedures indicate that the transfer form should indicate the reason, receiving facility, accepting physician, and patient acknowledgement of the transfer. Completed forms document compliance with Emergency Medical Treatment and Active Labor Act (EMTALA) regulations.

ED nursing reports are not consistently completed in accordance with departmental procedures. Of the ten ED visits reviewed, admitting diagnosis was omitted for two patients, and vital signs were not recorded for one patient. Additionally, a nursing report was not completed for one patient.

Management Plan - Management will perform the following actions to ensure transfer forms are completed appropriately by ED attending physicians:

- Review requirements and current compliance with Emergency Medicine faculty
- Provide feedback to transferring physician if form is not completed
- Management has also established the following plan to reiterate documentation standards with ED nursing staff by reviewing guidelines with the ED nurse manager, reviewing requirements and current compliance with ED nursing staff, establishing a continuous quality improvement process to monitor admit form compliance and completion, and providing feedback to admitting nurse when form is not completed or is missing information.

The U-M Emergency Department has established a strong control environment. University Audits will conduct a follow-up review in the second quarter of fiscal year 2009 to assess progress on action plans.

Patient Privacy Audits

#2008-401

Issued May 28 2008

University Audits reviewed patient privacy policies, procedures, and practices at the following health care units:

1. U-M School of Dentistry (UMSOD)
2. University Health Service (UHS)
3. Institute for Human Adjustment (IHA) Centers
 - a. University Center for the Child and Family (UCCF)
 - b. University Center for the Development of Language and Literacy (UCLL)
 - c. Psychological Clinic
4. U-M School of Nursing Nurse Managed Centers (UMSONNMC)
 - a. North Campus Family Health Services

- b. Community Family Health Center
- 5. U-M Autism and Communication Disorders Center (UMACC)

These organizations are outside of the University of Michigan Health System (UMHS) and provide patient services, manage patient health information, and bill for services. They are defined and designated as health care components of the University of Michigan, a covered hybrid entity regulated by the Federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), and as such are subject to the HIPAA Privacy Rule. The Privacy Rule establishes minimum federal standards for safeguarding the privacy of individually identifiable health information and confers certain rights to individuals, including rights to access and amend health information and to obtain a record of when and why protected health information was shared with others. In addition, the State of Michigan has certain privacy rules not covered by HIPAA.

The audit was performed in collaboration with the UMHS Privacy and Compliance Office to assess compliance with federal and state privacy rules for non-UMHS health care units. The UMHS Privacy and Compliance Office provides on-going oversight and monitoring of patient privacy practices at UMHS, therefore, UMHS is not part of the scope of this audit.

University Audits:

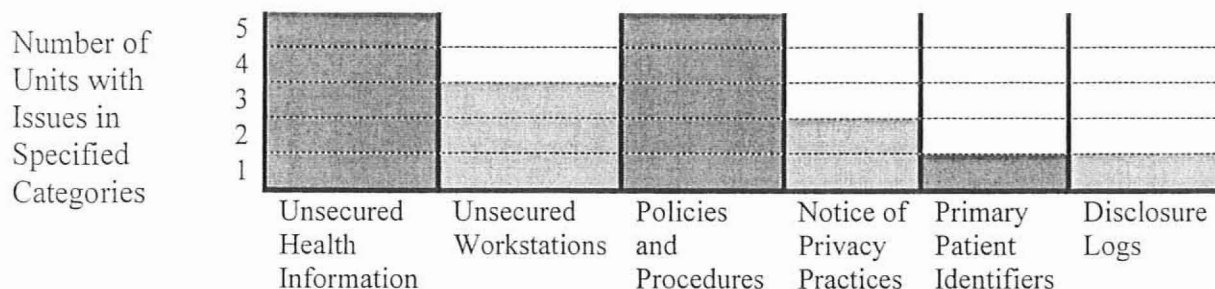
- Reviewed privacy control self assessments developed by University Audits and completed by personnel from individual units
- Worked with unit privacy delegates to review and assess unit policies, procedures, forms, privacy notices, and educational practices
- Substantiated compliance using sample testing
- Performed a walkthrough of health centers and observed management of protected health information

The audit identified a number of good practices used by one or more of the units to safeguard health information and decrease the risk of accidental disclosure. These practices include:

- Modified Check-in Process - Any of several processes (i.e. electronic check-in, verbal check-in, etc.) that prevents unauthorized individuals from seeing the names of patients who have already checked-in.
- INITS Coding - A system using parts of patient names (instead of whole names) to identify the patient. For example, a coding system that uses the first four letters of the last name and the first two letters of the first name would identify John Smith as SMITJO. (Rules for altering the names of patients whose last names have less than five letters are slightly different.)
- Sound Blocking - Use of white noise (i.e. sound machines, piped-in music), sound baffling between walls, or sound deadening materials on walls to prevent individuals from overhearing conversations at check-in desks, in treatment/examination rooms, and other locations.
- Special Signage - Use of posted signs to 1) remind patients, interns, and staff that private discussions should not be held in public locations; and 2) request that patients waiting in line maintain a specific distance from patients at the check-in desk.
- Closing Checklist - Checklist describing specific actions to take before closing health centers for the day. Checklists can also be used to identify specific actions that individuals should take before leaving the office for the day.
- Cover Sheets - Use of blank sheets of paper to cover patient schedules to decrease the chance that unauthorized personnel accidentally view private information.

University Audits prepared individual management advisory memorandums for unit administrators listing detailed audit issues and recommendations, and management's action plans for addressing audit issues. The chart below summarizes significant audit concerns and illustrates the number of units in which these concerns were noted. The Detail of Audit Findings lists specific issues associated with audit categories noted in the Summary of Audit Findings Table.

Summary of Audit Findings



Note: Health care units with more than one clinical area are treated as one facility.

Opportunities for Improvement

The following improvement opportunities were discussed with health care unit administrators:

- Develop procedures to change keypad combinations periodically.
- Ensure all personnel, including students and volunteers, receive privacy training. Ensure staff and students are aware of approved methods of discarding documents containing protected health information.
- Monitor the effectiveness of training by performing periodic walkthroughs of clinical facilities to determine if personnel understand and practice privacy policies and procedures.
- Develop, document, and implement computer security lockout policies and procedures to reduce the risk of accidental disclosure. Enable automatic password-protected screen savers.
- Develop and document privacy policies and procedures and keep them up-to-date. Ensure existing and new employees understand new and revised policies.
- Ensure that the Notice of Privacy Practices is prominently posted on the unit's website and at the facility.
- Strengthen controls over primary patient identifiers and other sensitive information by tightening disposal procedures and ensuring workstations are locked when not attended.
- Ensure all disclosures of protected health information are logged.

UMHS Privacy and Compliance Office personnel will continue to work with health care units to help them meet privacy requirements. University Audits will perform unit-level follow-up reviews to assess the progress of unit-level action plans.

University of Michigan Hospitals and Health Centers Social Work Gift-Funded Programs

#2008-804

Issued May 29, 2008

University Audits performed an audit of the internal control structure of the University of Michigan Hospitals and Health Centers (UMHHC) Department of Social Work gift-funded programs. The Department of Social Work administers multiple assistance programs for patients and their families. Financial support for these programs comes primarily from donated gifts. The Guest Assistance Program, a sub unit of Social Work, coordinates and distributes the support on a needs-based eligibility assessment. Examples of the type of assistance to qualified patients and their families include:

- Financial assistance for transportation, parking, and lodging
- Emergency meal, grocery and other limited financial assistance
- Help with arranging transportation and lodging
- Coordination with Children's Special Health Care Services and Department of Human Services
- Maintaining a supply of donated wigs and other head coverings for cancer patients

The Guest Assistance Program also administers assistance programs on behalf of Child and Family Life, Mott Community Relations, and the Cancer Center. They have recently been approached by the Trauma and Burn Center and the Transplant Center, among others, to administer unit assistance programs.

The scope of the audit was gift-funded receipts and disbursements for patient and family assistance, primarily managed by the Guest Assistance Program of the Department of Social Work.

The Department of Social Work has developed a strong system of controls for monitoring patient assistance. Notable features include:

- Electronic tracking and control of gift cards and other items of monetary value, such as lodging vouchers
- Tracking of patient assistance by patient ID (allowing social workers to monitor for trends or patterns of overuse)
- Real-time tracking and management approval of patient assistance expenditures made through a variety of payment mechanisms, including gift cards, petty cash, P-CARDS and non PO vouchers
- Ability to develop detailed community benefit reporting for management, donors, and external agencies

Control Issues:

- P-Card Multiple Users - Social Workers and Patient Services Assistants in the Guest Assistance Program and other department-managed areas routinely use the same P-Card for procuring gift cards, lodging, transportation, and other services. *U-M Standard Practice Guide 507.1 Purchasing* indicates that only the cardholder is responsible for the proper use of the card and only the cardholder should use the P-Card. Usage by individuals other than the cardholder can lead to misuse, a lack of accountability, and difficulty assigning responsibility for questionable charges.

Management Plan - All Guest Assistance Staff with procurement duties have submitted paperwork for individual P-Cards. Appropriate P-Card training will be scheduled for each staff member as part of the P-Card activation process.

- P-Card Reconcilers and Approvers - The department's Senior Administrative Specialist averages approximately \$10,000 a month in P-Card expenditures and also reconciles that P-Card statement. University policy recommends that the role of P-Card holder and reconciler be separate. In addition, the P-Card statement of the Department Director is approved by the Department Administrative Manager. University policy requires the P-Card approver to be of a higher administrative authority than the P-Card holder.

Management Plan - The Senior Administrative Specialist's expenditures are now reviewed by her direct supervisor and the Department Director's expenditures are approved by the Chief Administrative Officer. **This issue is closed.**

- Gift Receipt Processing - Some donations and fundraising receipts are received directly by Social Work staff. These funds, in the form of checks and cash, are given to the Department Administrative Specialist for processing. Normally, for donations, the Administrative Specialist fills out a gift processing form and delivers the funds to the Office of Gift Administration, for further processing and deposit to a restricted gift account. During our limited testing, University Audits noted a \$1,492 donation from a local church designated for Mott Children's Hospital that bypassed normal gift processing and was deposited to auxiliary fund 56000 instead of gift fund 30000. Social Work administrative staff explained that the funds were designated for the purchase of toys for Mott Children's Hospital on an administrator's P-Card. All gifts need to be processed through Gift Administration, so that the donor information is appropriately reported for tax purposes and an official donor receipt is generated.

Management Plan - Due to the relatively low dollar amount and small number of staff directly handling cash receipts, it may not be feasible to segregate logging receipts and form preparation duties, but cash receipts will be logged and reconciled to the monthly Statement of Activities. Staff preparing deposits of receipts will be educated about the importance of appropriate crediting and acknowledgement to the donors. Expenditures related to any designated funds received will be charged to the fund where the cash is received so that proper matching of revenues and expenditures occurs. Fund 56000 cash receipts will be reviewed for fiscal year 2008 and corrections, if needed will be made before fiscal year-end.

- Emergency Funds - Hospital Cashier's office limits petty cash reimbursements to \$200 per individual per day. Occasionally, due to urgent patient assistance needs, Social Work must issue several individual \$200 petty cash vouchers in one day, or over several days to circumvent the \$200 a day limit. Emergency cash needs are for patient basic needs, such as housing, allowing the patient to be discharged to a safe environment.

Management Plan - Management will work with UMHHC Cashiers and Financial Operations to develop workable solutions to funding emergency needs.

- Database Documentation - Social Work does a good job of tracking patient assistance payments. University Audits detected no excessive payments to individual patients, and there is adequate documentation of demonstrated need. Assistance granted is consistent with donor restrictions. During testing of several months of transactions, UA noted three instances where daily limits on gift cards to individuals were exceeded without documented evidence of required manager approval. In addition, several limited sequence gaps in numerically controlled gift cards were noted, but there was no indication of abuse or an overall problem.

Management Plan - The Guest Assistance Program has instituted weekly monitoring reports to detect and follow-up with staff on documentation concerns. **This issue is closed.**

- Policies and Procedures - The Guest Assistance Program has written policies for providing assistance to patients and family members. These policies are based on a variety of criteria, including funding source, demonstration of need and type of assistance. During our recent audit, we noted that some of the guidelines were out of date and did not reflect current practice.

Management Plan - Management will review and update all guidelines and criteria for providing patient assistance.

University Audits will follow up on the status of action plans during the first quarter of fiscal year 2009.

FOLLOW-UP REPORTS

University of Michigan Computing Environment Kerberos Passwords and Uniqname

#2007-304

Original Report issued June 22, 2007

Follow-up Report issued May 9, 2008

Disaster Recovery Plan:

During the original audit, it was noted that no formal Disaster Recovery Plan (DRP) existed for Kerberos. UMCE indicated that Information Technology Central Security had been working on a DRP for pandemic flu. This was to be the basis for building the Kerberos DRP.

Since the audit was completed, UMCE has increased the system documentation available online, has addressed business continuity in the event of disaster, and has reduced their projected recovery time. These are all

significant steps toward the thorough and complete DRP they are building. Based upon completion of all of these milestones, it is clear the required DRP will be completed.

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

ROTC Business Office Internal Control Review Audit Follow-up – Army Review

#2007-818

Original Report issued September 11, 2007

Follow-up Report issued May 23, 2008

University Audits conducted a follow-up review of the ROTC Business Office - Army to confirm:

- Adequate training for individuals with delegated signing authority
- Appropriate review and approval of P-Card, Non-PO voucher, and Travel and Hosting expenses
- Monthly reconciliations of the Statement of Activity (SOA) and Gross Pay Register (GPR)
- Documented procedures for training requirements, procurement processes, and reconciliations

Army ROTC made significant progress toward addressing recommendations made during the audit. However, the reconciliation and procurement processes have opportunities for improvement and procedures still need to be documented.

- Delegation of Authority - Individuals with procurement responsibility and approval authority are receiving training to obtain sufficient knowledge of University guidelines. Training requirements will be included in documented procedures. **This issue is closed.**
- Purchasing and Travel and Hosting Policy and Procedure - Management made progress with ensuring that procurement processes are consistent with University guidelines. All transactions reviewed were approved by the appropriate higher authority; however, travel and hosting documentation was not consistently completed, and the P-Card guidelines were not consistently followed. Management will document purchasing policies and procedures, including travel and hosting. During the second follow-up, University Audits will review documented procedures and verify adequate procurement processes.
- SOA and GPR Reconciliation - The Academic Secretary reconciles the SOA monthly. The Assistant Chair will begin to reconcile the GPR to source documentation on a monthly basis. Management will document reconciliation processes. During the second follow-up, University Audits will review documented procedures and the GPR reconciliation.

University Audits will conduct a second follow-up of Army ROTC business office internal controls during the first quarter of fiscal year 2009.

As part of this follow-up, University Audits also reviewed processes at the Navy and Air Force ROTC offices to confirm that the appropriate internal controls are in place:

- Adequate training for individuals with delegated signing authority
- Appropriate review and approval of P-Card, Non-PO voucher, and Travel and Hosting expenses
- Monthly reconciliations of the Statement of Activity (SOA) and Gross Pay Register (GPR)
- Documented procedures for training requirements, procurement processes, and reconciliations

Results of those reviews are shown below.

Due to recent changes in key personnel, current Air Force ROTC personnel were not fully aware of the initial audit recommendations to Army ROTC until the time of the follow-up review. Management is in the process of documenting training, procurement, and reconciliation procedures. Current practices include the following:

- Delegation of Authority - Individuals with procurement responsibility and approval authority are receiving training to obtain sufficient knowledge of University guidelines. Training requirements will be included in documented procedures. **This issue is closed.**
- Purchasing and Travel and Hosting Policy and Procedure - P-Card, Non-PO voucher, and Hosting expenses reviewed were adequately approved and processed consistent with University guidelines. Management is considering a few options that will help ensure that reconciled/approved P-Card statements are submitted to Procurement Services timely. Management will document purchasing policies and procedures, including travel and hosting. During the second follow-up, University Audits will review documented procedures and verify timely submission of reconciled P-Card statements.
- SOA and GPR Reconciliation - The Administrative Assistant Intermediate reconciles the SOA monthly. The Chair reconciles the GPR to source documentation on a monthly basis as well. Management will document reconciliation processes. During the second follow-up, University Audits will review these documented procedures and confirm that timesheets are signed by the appropriate higher authority before time is entered into the system.

University Audits will conduct a second follow-up in the first quarter of fiscal year 2009.

Navy ROTC practices and procedures adequately address all recommended internal controls. Current practices include the following:

- Delegation of Authority - Individuals with both procurement responsibility and approval authority are receiving training to obtain sufficient knowledge of University guidelines. Management has documented training requirements.
- Purchasing and Travel and Hosting Policy and Procedure - Management is reviewing and approving travel, hosting, P-Card and non-PO transactions, in accordance with procurement guidelines. Travel budgets and hosting limits are defined and monitored. Management has adequately documented purchasing procedures, including travel and hosting.
- SOA and GPR Reconciliation - Management is reconciling and monitoring the SOA and GPR on a monthly basis and has agreed to include a detailed comparison to time reports in the GPR review. Management has documented reconciliation and monitoring procedures.

We recommend that these and other business office internal controls be reviewed and updated regularly. **The Navy ROTC review is closed.**

The first follow-up report was issued on January 31, 2008. A second review was conducted to determine if the remaining issues have been adequately addressed by management.

- Persistence of Login Sessions - Unlike other CoSign-enabled U-M services such as Wolverine Access, users logging out of CoSign (Weblogin) were not being logged out of CTools. In January, a notice advising users to quit the web browser in order to fully terminate their CTools session was posted on CTools as an interim safeguard.

The CTools Implementation Group has included reprogramming of the CoSign implementation in its FY09 budget. This group hired a new programmer in April who will be assigned to this project, and will establish a target date for completion of the CoSign work after additional conversation with ITCS CTools Operations. To ensure sufficient testing and adhere to the CTools release schedule (July and December), the group estimates the improved logout function will be activated Winter Term 2009 (January 2009). The interim user-warning message will remain in place on the CTools home page until the improved logout function has been activated. Based on these commitments and the progress they represent, this issue is closed.

- Log Review - CTools logs were not used to proactively identify unusual or abnormal activity in CTools. CTools Operations (CTOps) has developed a number of statistics derived from CTools system logs and web server logs that measure performance and load on the system. Management is now provided a snapshot of a dashboard depicting these measures both numerically and graphically. Several of these statistics will be used by the CTools Implementation Group or CTOps to identify abnormal activity. For example, if the activity impacts performance, applicable statistics include the number of established connections, number of client requests, memory and CPU consumption, and database queues. In addition, the tool-by-tool analysis of HTTP status codes indicating success or failure – could be used to identify targeted attacks. This issue is closed.
- SLA between ITCS and Digital Media Commons - At the time of the initial audit, the service level agreement (SLA) between ITCS and Digital Media Commons (DMC) was outdated and unsigned.

Because of their complexity and the effort required to provide them, these services were identified by both organizations as the most important area in which to standardize expectations, processes, and procedures. In response to the need for standardization, ITCS and DMC have developed a draft outline of a SLA for testing, piloting, and prototyping of CTools software. University Audits reviewed the draft outline and found it to be thorough. It identifies a number of developer needs, control requirements, and support limitations that must be addressed in the SLA. Management maintains that a comprehensive SLA update remains a priority for the redesigned CTools governance group. This issue is closed.

- Upgrade Approval Process - The process through which the CTools Advisory Committee (CTAC) authorizes upgrades to new releases of CTools has not been consistently followed. During the first follow-up it was noted the Vice Provost for Academic Information was planning to establish a new CTools governance board by fall 2008.

Management has proposed to the Vice Provost for Academic Information an expanded interim advisory group replacing CTAC to review and approve the summer 2008 CTools release. A more complex permanent governance structure has also been proposed. University Audits reviewed the proposal draft

detailing these organizational changes. This redesign of CTools governance encompasses a renewed focus on stakeholder review and approval of major CTools releases. This issue is closed.

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

Michigan Public Media – Phase II
Original Report issued April 24, 2006

#2006-806
Follow-up Report issued May 29, 2008

An initial follow-up review was completed and reported on May 10, 2007. In that follow-up review, University Audits determined management had made progress towards a stronger control environment by implementing recommendations regarding:

- Assessment of leadership performance and responsibilities
- Management of premium gifts
- Inventory practices
- Grant management
- Conflict of interest
- Relationships with third parties
- Allegiance and security rights

However, there were remaining issues that required additional action by management. During the current follow-up, University Audits verified management has satisfactorily implemented corrective action for all remaining issues. **This audit is closed.**

- Accounting Oversight and Support - As noted in the previous follow-up, Management drafted policies clarifying MPM account oversight, monitoring controls, and appropriate segregation of duties. Improvements were made immediately after the first follow-up to the reconciliation processes for P-Card statements and the Statements of Activity.

A process to reconcile gift revenue from MPM's Allegiance System to the Office of Development's (Development) DAC system was recently implemented. MPM installed an upgrade to the Allegiance system and has worked with Development to obtain their unique identification number for each donor. Development's unique identifiers were input into the Allegiance system for each MPM donor. Monthly, gifts will be electronically compared from Allegiance to DAC. Gifts that are not automatically matched by the electronic comparison by the following month will be manually investigated. The Media Financial Officer will review the reconciliation each month. This reconciliation process continues to be refined to reduce manual investigations of unmatched gifts between Allegiance and DAC.

- Financial and Operational Policies - During the previous follow-up, University Audits noted that policies and procedures for key activities at MPM had been formalized and distributed to staff. These policies were also accessible electronically via the "common" drive. The information on this drive included superseded versions of policies which might cause confusion; University Audits suggested that superseded versions be maintained in a separate file for historical purposes. Management continues to document and update detailed procedures for specific functions, as changes occur. In order to reduce the risk that superseded versions of policies and procedures are accessed and relied upon by staff, management has removed the policy manual from the "common" drive until significant revisions are complete. Hard copy manuals have been distributed to all managers and supervisors and are easily accessible by staff.

In addition, management has reviewed Standard Practice Guide sections 201.86 "Services of Independent Consultants" and 507.4 "Independent Consultants" and determined these standards provide sufficient

guidance to address the needs of MPM. The MPM policy manual contains directions to consult these SPGs for guidance regarding independent consultants.

- Pay Practices - Management previously established new procedures for the proper authorization and handling of time reports and the tracking of off-site work. In addition to these improved procedures, MPM has begun performing detailed comparisons of the Gross Payroll Register to actual time documents.
- Business Continuity - In the previous follow-up, University Audits noted MPM had increased physical security to the premises of the station and developed a very thorough and detailed Pandemic Preparedness Plan that would address issues arising from an influenza, or similar epidemic. In April 2008, management completed a disaster recovery and business continuity plan that addresses data, program, transmitter, satellite, and equipment failures, and losses.

Ross School of Business Dean's Office – Fiscal Responsibilities Audit

#2007-821

Original Report issued July 20, 2007

Follow-up Report issued June 13, 2008

The original report identified improvement opportunities related to procurement processes, Ross Marketplace operations, Statement of Activity (SOA) and Gross Pay Register (GPR) reconciliations, and delegations of authority. University Audits performed a follow-up review to assess the status of management's action plans.

Ross School of Business (RSB) management has adequately addressed concerns raised during the audit. See summaries below for additional information. **This audit is closed.**

Procurement Processes:

RSB management has implemented several processes to improve the controls related to the procurement process:

- The Assistant Dean for Finance and Planning reduced the number of P-Cards for which he is the primary approver from 63 to 24.
- The Senior Financial Specialist developed a Business Objects report that is being used to monitor P-Cards. The report monitors approval authority, spending trends and limits, and potential split transaction.
- University Audits did not identify any split P-Card transactions from the period February 7, 2008 through May 28, 2008.
- The Assistant Dean for Finance and Planning emphasized the importance of compliance with Procurement Services' guidelines to RSB staff, and provided a link to Procurement Services' website. The communication highlighted the following areas:
 - Unallowable P-Card uses
 - Timely processes of reconciled P-Card statements
 - Supporting receipts for P-Card expenses
 - Appropriate chartfield combinations, including indirect cost recovery excluded items
 - Adherence to the \$5,000 limit for P-Card transactions
- RSB uses the PeoplePay system for all non-appointment related payments to individuals.
- Based on a sample of procurement expenses, travel and hosting documentation appears to be consistently included in support documentation, and indirect cost recovery excluded expenditures appear to be flagged with the appropriate class.

Ross Marketplace:

Marketplace processes were updated and documented to improve cash handling, credit card processing and inventory management. The sales revenue being used as an unauthorized change fund was deposited, and a proper \$100 change fund was obtained through Accounts Payable.

RSB decided to outsource the management of the online sales. RSB is considering several different options to continue to have merchandise available onsite. However, it is likely that the sales will no longer be managed by RSB staff. If Marketplace operations are outsourced, the issues identified in the report will no longer be relevant. RSB should re-assess the risks related to the new processes and address them as appropriate. University Audits can assist in the review of new processes and procedures that are developed for the new outsourced arrangement.

Written Delegation of Authority:

Signing authority delegated by the Dean is now documented. Documentation includes the names and titles of individuals with delegated authority as well as the circumstances in which delegation is applicable. The delegations are signed by the Dean and the person accepting the authority. Delegates will be updated annually at the beginning of each new academic year, or upon position turnover by any of the individuals. The Dean will help assure compliance with University policies through periodic review of signing authority usage and reports from delegates.

Reconciliations:

The GPR and SOA were reconciled to source documentation for fiscal year 2008. Going forward, these reconciliations will be performed on a monthly basis.

Executive Education – Overtime Management:

Executive Education management updated the Overtime Approval Form to include the supervisor's estimate of overtime hours needed for the upcoming week and an explanation for any variances in actual overtime hours. Hours reported on time reports are reconciled to overtime calendars before time is entered into U-M's time reporting system to verify consistency and confirm that hours are reported on the actual day worked. A chart of anticipated overtime hours for each program is used to review the reasonableness of overtime charges and help balance the workload of the program assistants. Executive Education management estimated a 34% reduction in overtime expense for fiscal year 2008, based on the first half of the year.

Biomedical Research Core Facilities Financial Internal Controls

#2007-826

Original Report issued October 23, 2007

Follow-up Report issued June 25, 2008

University Audits recently performed a follow-up review of BRCF management corrective action plans. Management has addressed the issues appropriately as described below. **This audit is closed.**

Accounting for Capital Equipment: Interest paid on Medical School loans to finance equipment for the DNA Sequencing and Flow Cytometry Cores was reimbursed to BRCF in full. BRCF and Financial Operations management corrected accounting procedures for depreciation and equipment.

Segregation of Financial Transaction Duties:

- Billing—Segregation of responsibilities for price list content, billing input, and billing data upload to the M-Pathways system is in process. The MSIS applications developer that created the proprietary BRCF billing application is separating access privileges for billing from access to the product data, including price. The target date for completion is July 7, 2008.
- Procurement—The BRCF Director is performing a review of individual statements of activity transactions on the one department account where a concentration of duties exists in the reconciliation and procurement processes. The Director reviewed system access and individual responsibilities for all BRCF administrative staff and determined that this concentration of duties does not occur for any other BRCF unit.
- Payroll—Core directors review the final approved paperwork for hiring new staff and personally deliver it to the appropriate HR office for processing. Employees no longer have access to their timesheets after they have been approved.

DNA Sequencing Services and Billing System:

- DNA propriety system documentation has been updated.
- Plans are well underway to move the DNA Sequencing server to a separate, secure location. One set of back-up tapes will be maintained at the current location, which will become the second data site. Additional data back-up and recovery will occur through a contractor data warehouse. Options for performing a complete restore in the new system will be investigated.
- The DNA Applications Programmer/Analyst Intermediate has performed both service unit and off-campus billings and will repeat the process in one to two months.
- The server doors are kept locked and the move to a more secure site is progressing as planned.

BRCF Policy and Procedure:

- Policy and procedures are being updated and documented.
- Security of supplemental spreadsheets was reviewed by the University Audits IT team and separate recommendations to improve the internal control environment were made. BRCF best practices and opportunities for improvement were documented and shared with BRCF management.

Recommendation for assessing opportunities to automate supplemental spreadsheets through M-Pathways system reporting will be passed to an interim or new BRCF Director upon the current director's retirement at the end of July 2008.

University Audits – University of Michigan
Open Audits Follow-up Table
June 30, 2008

Audit Title	Report Date	Issues	Expected Completion
Information Technology Central Services Software Licensing and Distribution Billing Systems and Practices 2007-106	2/7/08	Documentation of procedures for licensing negotiations and billing	October 2008
School of Dentistry HIPAA IT Security 2008-308	6/19/08	Security Policy; Personal Storage of EPHI	September 2008
UMH Operating Rooms – University Hospitals Supply Chain Management 2007-108	8/17/07	Product recall follow-up; consistent and documented inventory practices; and conflict of interest communications	August 2008
University of Michigan Health System Human Resources Fiscal Responsibilities 2008-209	1/21/08	Payroll management; documentation of processes	August 2008
University of Michigan Health System Offsite Professional Contracts 2008-111	2/29/08	Documentation of business practices for renewal of contracts; evaluations of physician assistants	September 2008
University of Michigan Hospitals and Health Centers Emergency Department 2008-112	05/09/08	Training Action Plan	December 2008
Patient Privacy 2008-401	5/28/08	Policies and Procedures; training	December 2008
University of Michigan Hospitals and Health Centers Social Work Gift-Funded Programs 2008-804	5/29/08	P-Card multiple users; P-Card reconcilers and approvers; gift receipt processing; emergency funds; database documentation; policies and procedures	September 2008
Plant Operations Zone Maintenance Purchasing Controls 2007-812	4/24/07	Purchasing. New methods for handling inventory receiving and tracking	First follow-up was completed December 2007
			Second follow-up July 2008
Matthaei Botanical Gardens & Nichols Arboretum, Business Office Internal Control Review 2007-817	6/19/07	Strengthen cash handling procedures; instructor payments; credit card refund controls; remove unnecessary sensitive data in files. We will observe and review the annual plant sale in May 2008	July 2008
Intercollegiate Athletics Academic Support Services 2007-408	7/18/07	Student counseling practices; employment and payroll controls; staff training and development	September 2008
Intercollegiate Athletics NCAA Compliance – Student-Athlete Equipment and Apparel 2007-409	8/24/07	Record retention	July 2008

Audit Title	Report Date	Issues	Expected Completion
Army ROTC Business Office Internal Controls 2007-818	9/11/07	Orientation training for new Army Executive Officers to include: University purchasing, hosting, traveling, and reconciliation processes	First Follow-up completed May 2008
			Second Follow-up (Army and Air Force) September 2008
University Human Resources Family and Medical Leave Act 2007-403	12/17/07	Training; update relevant SPG sections; written notifications	July 2008
Ross School of Business Multidisciplinary Action Projects 2007-103	1/10/08	Travel registration; procurement; expendable restricted funds; documented procedures	September 2008
Transportation Services 2007-101	1/28/08	Controls over physical access; system user access levels; commercial driver's license testing; vehicle inventory monitoring; fuel inspection upon delivery; gross pay register review; imprest cash fund; formal policies and procedures	September 2008
I-9 Employment Verification Process 2007-823	1/29/08	Filing timeliness; automation; training	September 2008
U-M Dearborn Office of the Provost Fiscal Responsibilities 2008-204	3/19/08	Fairlane Center: Approved recharge rates; deposits	July 2008
Office of the Vice President for Communications Fiscal Responsibilities 2008-211	5/29/08	Segregation of duties; delegation of authority; cash deposits	September 2008

