

THE UNIVERSITY OF MICHIGAN

REGENTS COMMUNICATION

Item for Information

Received by the Regents  
January 17, 2008

Subject: Report of University Internal Audits  
October 2007 – November 2007

Background:

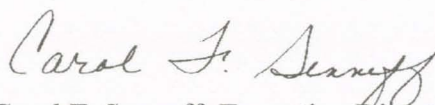
This is the report of the Office of University Audits activities for the period **October 1, 2007 through November 30, 2007**. The summaries of audits contained in this report were previously reported to members of the Regents' Finance, Audit and Investment Committee and included in discussions at Committee 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 **November 30, 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](mailto:csenneff@umich.edu).

Respectfully submitted,



Carol F. Senneff, Executive Director  
University Audits

## **ORIGINAL REPORTS**

### **Campus**

#### **Intercollegiate Athletics NCAA Team Travel**

#2007-412

Issued October 10, 2007

The objective of this audit was to assess internal controls governing team travel activities to determine if controls are sufficient to ensure team travel expenditures comply with NCAA, University, and departmental policies. To meet this objective, University Audits:

- Reviewed NCAA regulations, University, and Intercollegiate Athletics (ICA) policies and procedures to determine acceptable practices
- Interviewed staff in the Athletic Business Office and Compliance Services Office to:
  - Determine if they had a sufficient understanding of NCAA, University, and ICA travel guidelines
  - Identify training activities undertaken to ensure that coaches understand rules and regulations associated with team travel
  - Identify activities undertaken to control and monitor team travel expenditures
- Reviewed cash controls to determine if cash advances were reconciled and accounted for appropriately
- Performed detailed transaction testing to determine if team travel activities complied with NCAA, University, and ICA guidelines

#### **Cash Control Issues:**

- 1.1 **Justification for Cash Advances** - University Audits tested a sample of travel expense vouchers (TEVs) and noted cash advances well in excess of travel requirements. Significant amounts of cash are used for purchases that should be charged to University purchase cards (P-Cards). For example, one TEV revealed that approximately \$2,800 was paid in cash for meals that could have been charged to a P-Card. On average, approximately half of travel advances sampled had significant balances returned to the department, with returns ranging from 20% to 70% of the original advance.

**Management Plan** - ICA will track cash returns against advances to better monitor which advances appear to be larger than necessary. ICA will educate those coaches/administrators about the risks of excessive cash advances and amend its travel policy to emphasize the need to keep team travel cash advances reasonable. The Athletic Business Office (ABO) will challenge cash advance requests that appear unreasonable and will continue to work with coaching staffs as needed to assist them in determining cash needs for travel. In doing so, the Athletic Business Office will be mindful that a certain amount of flexibility in projecting cash needs is required, particularly for larger parties where there is uncertainty relative to the trip itinerary and meal plans.

- 1.2 **Promissory Notes** - The ABO can directly issue cash advances to employees through a special banking arrangement authorized by U-M Treasurer's Office. A review of cash advances revealed that ABO personnel do not require coaches to sign promissory notes for cash advances to acknowledge:
- Receipt of the advance
  - Responsibility to account for the advance within 30 days after return
  - University's rights to recover funds directly from the person requesting the advance

University Standard Practice Guide section 501.4-1 states, "The traveler/host requesting the advance must sign a non-interest-bearing promissory note for the amount of the advance."



**Management Plan** - ICA will incorporate a promissory note on a travel advance check envelope. Travelers will be asked to sign the envelope/promissory note when travel advance checks are picked up in the Travel Office.

- 1.3 Segregation of Duties Over Cash Handling - The ABO does not have adequate segregation of duties over processes for accounting for team travel expenditures. The employee responsible for reviewing Travel Expense Vouchers (TEV) is also responsible for accepting payments for unused portions of cash advances. Payments are often returned in cash.

**Management Plan** - Upon final review of each Travel Expense Voucher (TEV), the Business Office Manager (or Assistant Athletic Director in his absence) will review the TEV for unusual corrections or alterations, and trace the deposit to the Cash Receipt Ticket Confirmation. The deposit ticket number will be recorded on the TEV during the final review.

Travel Expense Vouchers Control Issues:

- 2.1 Lack of Complete Documentation and Review - University Audits noted several documentation issues while reviewing travel documents, including one travel expense voucher (TEV) that did not include the travel squad list needed to review the reasonableness of expenses, and two TEVs that were not signed by the head coach. University Audits also noted one hotel statement that may have overcharged a team for an additional room during their visit. The individuals reviewing the TEV did not have sufficient information to determine how many hotel rooms should have been billed each night.

Individuals reviewing travel documents should have sufficient information to ascertain the appropriateness of expenditures. University Standard Practice Guide states that travelers must provide travel reports to substantiate amounts, dates, use, and business purpose of expenses to meet the Internal Revenue Services requirements for an "accountable plan".

**Management Plan** - ICA will develop a checklist for use during the review of travel expense vouchers and supporting documentation. The checklist will contain the documents that reviewers should have prior to performing the review and what should be reviewed prior to approval. ICA will also develop an educational checklist for coaches and administrators responsible for team travel, which will highlight important policies, procedures, and helpful hints, to minimize and appropriately account for travel expenses.

- 2.2 Meal Per Diems - During a review of travel expenditures, University Audits noted that:
- Meal per diems occasionally exceeded departmental meal allowances
  - Per diem lists provided by coaches do not always list the meal for which cash was provided, which often makes it impossible to determine whether the per diem exceeds ICA limits
  - Individual meals for coaching staff who could not attend group meals exceeded meal allowances
  - Per diem lists did not always identify the individual's affiliation with the University (e.g. student-athlete, student trainer, asst. coach, etc.)

When coaches elect to provide per diem to student-athletes in place of meals, NCAA regulations require all student-athletes to receive identical amounts. Per diem lists should provide sufficient information to ascertain whether ICA and NCAA guidelines have been met.

**Management Plan** - The Compliance Services Office revised the Travel Squad/Per Diem List for fiscal year 07-08 team travel. The revised form requires coaching staff to list the daily amount and meal provided on the form. In addition, the Athletic Business Office travel policy will be revised to provide more guidance about documenting per diem amounts as well as the travel party listing.

Special exceptions to the per diem limits will be documented and approved by the appropriate sport administrator.

University Audits will perform a formal follow-up review in the third quarter of fiscal year 2008 to assess the progress of action plans.

### Information Technology

#### Occupational Safety and Environmental Health – Hazardous Materials Online Tracking #2008-311

Issued October 11, 2007

The Department of Occupational Safety and Environmental Health (OSEH) is the department within Facilities and Operations that supports the U-M community by promoting health, safety, protection of the environment, and regulatory compliance.

The OSEH Hazmat database administrator designed, built, and administers the online tracking database. The database was created using Microsoft Access. It uses a series of macros to perform required functions. It resides on a server and Storage Area Network (SAN) administered by Business and Finance Information Technology (BFIT). These systems are stored in the Medical Center Information Technology machine room at Arbor Lakes.

The purpose of this audit was to review controls in place to protect the integrity of the Hazmat online tracking database. Controls related to both the database itself, and its computer systems housing were reviewed, evaluated, and tested. Review of BFIT's controls was done at a high level.

The audit scope included review and testing of:

- User access to the database
- User permissions within the database
- Procedures and practices directly related to the database
- Security of systems housing the database

No significant issues were found in the review of the Hazmat online tracking database. The combination of BFIT's diligent system administration, a well designed and maintained database interface, and good business practices and procedures contribute to the well controlled environment.

No follow-up is necessary. **This audit is closed.**

#### Michigan Administrative Information Services – eResearch

#2007-302

Issued November 26, 2007

University Audits performed an audit of application controls and change management processes in the eResearch information system supporting the administration of sponsored research at the University.

The primary purpose of the eResearch system is to simplify the review of research involving human subjects, and improve oversight of the process through standardization and automation. SPG Section 303.5, based on numerous government regulations and ethical guidelines, requires that any research project involving human participants be either approved or exempted in advance by an Institutional Review Board (IRB). Researchers planning any of U-M's approximately 7,000 projects involving human subjects<sup>1</sup> apply for IRB review using a standard eResearch form. Application materials, reviewer decisions, comments, questions, and revisions are all sent and received within eResearch. The system enables tracking of completion status and maintains an audit trail of user activity to further support compliance efforts.

---

<sup>1</sup> Parnes, M.G, "eResearch: University of Michigan." Presented at Business & Finance Forum, February 8, 2007.



Additional eResearch objectives and functions include:

- Issuing reminders to promote timely application completion and review on both initial and continuing bases
- Improving timeliness of the reporting and review of adverse events and unanticipated problems encountered in the course of research
- Increasing workflow efficiency

Proposal and grant management capabilities are being developed as a second phase that will significantly expand the role of eResearch in the administrative process – not just for human subject research, but for all types of research. With this expansion, the University's dependence on eResearch will increase, as will the need for sound internal controls.

The eResearch system consists of commercial off-the-shelf application software from Click Commerce operating on a Windows server with Microsoft's SQL Server database and IIS web server. This system, as well as separate, dedicated development and quality assurance testing environments, is hosted by Michigan Administrative Information Services (MAIS). Users are authenticated via the CoSign service provided by Information Technology Central Services (ITCS). Interfaces are maintained with M-Pathways and the PEERRS training certification system. A subset of eResearch data is available in the Data Warehouse for reporting uses.

eResearch was developed and is managed by the MAIS Research Administration Systems team in partnership with the Office of the Vice President for Research (OVPR) and consultation with the IRB Council. The Phase I Lead Team, consisting of key personnel from MAIS, OVPR, and the IRBs, provides steering and leadership. The MAIS Research team also provides user training and support services to IRB staff, IRB members, and investigators.

University Audits' objective was to identify areas of information technology (IT) risk in the design, operation, and administration of eResearch, document the controls for managing them, and evaluate the effectiveness, expedience, and sustainability of the current controls.

We compared risks for eight COBIT<sup>2</sup> IT control activities relevant to the business and IT goals of this system. This analysis led us to focus the audit on application controls and change management, based in part on the uniqueness of these specific controls to eResearch.

The audit scope was limited to the eResearch application software, unique middleware, the integration of standard MAIS services, and other technical administrative processes performed by the MAIS Research team. It did not include the second phase of development involving proposal and grant management.

Through interviews, examination of documents, direct observation, analysis, and testing, we confirmed the presence, operation, and effectiveness of controls, and identified opportunities for improvement.

#### Control Issues:

1. Network placement of production server - All eResearch system components, application, web, database, and file services, are hosted on a single server due to vendor restrictions. To accommodate external user access requirements, the server was placed in the publicly accessible DMZ network. This does not conform to MAIS standards requiring servers accessing the internal storage area network (SAN) (as eResearch does for file and database storage) to be located in the access-controlled Secure Zone. This exception to policy was reviewed and approved by the MAIS Information Systems Security Officer prior to deployment, on the grounds that the eResearch server itself would not contain any sensitive or confidential data.

---

<sup>2</sup> *Control Objectives for Information and related Technology (COBIT) 4.1*. IT Governance Institute, 2007.

eResearch, however, does transact a small amount of data that could be sensitive, mostly pertaining to drugs under development. This data is processed by the eResearch server before being stored in files or in the eResearch database that are located on the internal SAN.

Hosts located in more highly exposed networks such as the MAIS DMZ are at greater risk of attack and compromise. If the eResearch server were compromised, the sensitive data it processes could be captured in transit. Temporary files, user upload directories, or test data sets containing sensitive information that are not periodically purged from the server could also be accessed.

**Management Plan** - MAIS Technical Information Operations (TIO) is planning to reconfigure the hardware architecture in conjunction with the deployment of eResearch Proposal Management. The new configuration will improve security by separating the database server from the web/application server and placing it in the Secure Zone network.

2. Required application items - Two items on the application form were marked "required" but did not have to be completed before successfully submitting the application. Normally an incomplete "required" item results in the system either refusing to allow the user to proceed to the next page of the application, or refusing to allow the application to be submitted.

Failure to enforce application requirements may impact the efficiency of the review process, as IRBs may not have all the information they need to render a decision, and applications may need to be returned to investigators for completion.

University Audits tested 100 of the greater than 400 items which could have been designated as "required" to ensure that failure to complete these items resulted in an inability to submit the application for further processing. Only two of the items tested failed to prevent successful submission of the proposal.

**Management Plan** - MAIS Research will amend the test plan to include validation of all required fields on all pages beginning with the December release. This will mitigate the risk in the future.

Based on the audit work conducted, University Audits has determined that IT controls support the integrity and availability of notification mechanisms, audit trails, certification checks, and the overall system.

The eResearch system and the MAIS Research team effectively leverage MAIS IT infrastructure and IT services. Server and database maintenance, and administration needs are fulfilled by MAIS specialists, and change management is integrated with standard MAIS processes. Based on prior audits of MAIS and observations of MAIS' general commitment to internal control, security, and most recently IT Service Management, integrating and leveraging these services is an important risk mitigation strategy.

A formal follow-up to the outstanding issues will be conducted in the third quarter of fiscal year 2008.

### Healthcare

#### University of Michigan Health System – Hospital Collection Agencies

#2007-112

Issued October 10, 2007

University of Michigan Hospitals and Health Centers (UMHHC) uses external collection agencies for collecting over-due accounts for patient services. External collection agency activities begin when accounts have at least one balance older than 90 days from bill date. Accounts are automatically transferred to pre-collection and collection agencies. Pre-collection is used prior to account delinquency and provides a friendly, early reminder that payment is now due or past due. Primary collection activities



commence once an account is delinquent and secondary collections activities begin once an account is delinquent for more than one year.

University Audits examined the following processes to evaluate the adequacy and effectiveness of financial and operational controls governing Hospital collections:

- Pre-collections
- Collections and secondary placements
- Account write offs
- Collection agency fees and payment posting
- Closed accounts

Control Issues:

- Collection Agency Fee Review - A review of monthly collection agency invoices and payments noted that no process exists to review the fees charged on pre-collection invoices. Adequate processes do exist for primary and secondary collections. Though no process exists, all pre-collection payments sampled appeared to be appropriate and within contract terms.

**Management Plan** - UMH Patient Accounts will develop a process to review the number of accounts transferred to the pre-collection agency then compare that number to the number of accounts for which UMHS is invoiced.

- Hospital Fee Collections - No review process exists to ensure that hospital accounts are transferred to the secondary collection agency after twelve months of inactivity with the primary agency. The primary collection agency contract states that all accounts that are inactive for twelve months are returned to U-M. At that time, hospital accounts in collection are transferred to the secondary collections agency. University Audits noted multiple instances of accounts that never transferred to the secondary agency or did not transfer timely.

**Management Plan** - A letter requesting prompt attention to this matter was sent to the primary collection agency. A monitoring process will be developed after the Health Quest upgrade in March 2008.

- Policies and Procedures Documentation - Hospital Billing does not have written documentation describing some of their business processes. Written policies and procedures should be in place to document activities, procedures, functions, responsibilities, and flow of information within a department to guide the daily operations and activities. Written policies and procedures are an integral part of a strong internal control framework and ensure continuity when there is employee turnover.

Hospital Billing Management should document key business processes and make them readily available to all personnel. Policies and procedures should be accurate, complete, and promptly updated when changes occur. The following policies and procedures should be formalized:

- Data transfer and balancing
- Collection agency invoice review and payment
- Account closeouts
- Account transfers from primary to secondary placement agencies

**Management Plan** - Formal policies and procedures will be developed for the activities listed above.

- Account Transfer Confirmations and Reconciliations - Hospital Billing electronically transmits accounts on a weekly basis to the collection agencies. However, confirmation is not received from the collection agencies to verify the data transmission was complete and accurate. Failure to

confirm and reconcile data transmission of accounts could result in a lack of collection activities performed on delinquent accounts. It is also a key component of ensuring the integrity and security of electronic protected health information.

**Management Plan** - Confirmation and reconciliation processes will be developed to ensure that collection agencies receive accurate and complete data for collection purposes.

A formal follow-up to address the outstanding issues will be conducted in the third quarter of fiscal year 2008.

**Medical School Biomedical Research Core Facilities Financial Internal Controls** #2007-826  
Issued October 23, 2007

The Biomedical Research Core Facilities (BRCF) provides specialized laboratory services to U-M researchers including direct and cost-effective access to research supplies, expert protocol development consultations, sophisticated and costly instrumentation, and highly trained professionals to perform protocols. Services are offered through six BRCF units: Biomedical Research Store, DNA Sequencing, Flow Cytometry, Protein Structure Facility, Transgenic Animal Modeling, and Biosafety Containment. Services are also provided to external researchers through Division of Research Development and Administration (DRDA) research grant sub-contracting and through professional peer networking.

The objective of this review was to evaluate the adequacy of financial internal controls that support accurate recording and appropriate transactions related to Core fiscal responsibilities, including recharge activities. The evaluation included the following financial areas:

- Recharge rate and billing processes for Protein Structure Facility and DNA Sequencing Cores
- Appropriateness and authorization of journal entries and transfers
- Appropriateness of accounting for equipment depreciation and service expense
- Payroll and purchasing controls
- Biomedical Research Stores inventory management
- Overall assessment of fiscal responsibilities control environment

Control Issues:

- Monitoring and Adjusting Recharge Rates - University Audits observed outdated and under-valued recharge rates in two BRCF units resulting in financial deficits. U-M Financial Analysis approved recharge rates are established to support Federal OMB A-21 direct cost requirements and University  $\pm 5\%$  breakeven policy.
  - The Protein Structure Facility accrued a \$900,000 deficit over a nine-year period without effectively revising their recharge rates to cover actual costs.
  - DNA Sequencing accrued \$43,000 of unbilled revenue for services rendered over a nine-month period while a new rate was developed. This resulted in untimely information to grant managers and the risk that research accounts billed at a later date may be closed.

**Management Plan** - The following actions resulted from a comprehensive rate review by the Office of Financial Analysis completed in June 2007:

- BRCF management and Financial Operations will both be monitoring and scheduling annual rate reviews from this point forward. If business plans or operations experience significant changes from projections, rate reviews will be scheduled at less than annual time frames on an as needed basis in order to comply with the expectation that variances greater than  $\pm 5\%$  are dealt with appropriately and in a timely manner.
- In April 2007 the Medical School transferred \$491,352.57 to the Protein Structure Facility internal service account to offset over 50% of the existing long-term accumulated deficit. The Medical School has committed to taking responsibility for covering the remaining



accumulated deficit associated with the Protein Structure Facility operation, including additional projected deficits that may accrue in fiscal year 2008.

- The DNA Sequencing Core accrual of unbilled revenue for services awaiting rate approval was a one-time incident. The Director of the DNA Sequencing Core understands that this procedure leads to the kind of issues noted and will submit rates for new services as the services become available rather than bundling them with an overall laboratory full rate review process.
- Accounting for Capital Equipment - Capital equipment purchases made in fiscal years 2003 and 2006 resulted in \$411,716 in direct costs to recharge rates while simultaneously contributing to indirect costs through depreciation. Depreciation was scheduled at less than the ten-year period stipulated by federal regulation. These costs included \$19,700 of interest payments to the Medical School in return for a loan to BRCF for purchasing the equipment. Federal reimbursement for sponsored research services through both direct and indirect costs for the same equipment is not compliant with Federal OMB Circular A-21, Cost Principles for Educational Institutions. Interest payments from the recharge accounts are also disallowed. BRCF discovered these issues in working through recharge rate approval renewal with Financial Analysis management in spring 2007 and are currently taking steps to remedy the errors.

**Management Plan** - With the assistance of Financial Analysis personnel, the following actions have been taken:

- The Medical School has reimbursed the appropriate internal service accounts for all interest paid as part of any equipment loan repayment.
  - Approved recharge rates will reflect corrected equipment depreciation recovery values and schedules of depreciation will be set to match the ten-year lifetime of instrumentation as required by cost-accounting standards.
  - Issues related to these past loans and repayments, and the required corrective actions, have been documented in a memo to the Medical School Finance Office. This memo was reviewed and approved by the University Office of Financial Analysis for accuracy and completeness. It will be the reference point for current action, as well as future policy and procedures, for capital equipment acquisitions that will be compliant with OMB Circular A-21.
  - University and Medical School Asset Management systems and equipment depreciation schedules will be monitored on an ongoing basis to ensure that the corrections applied to these issues are reflected accurately and future recharge transfers for depreciation are processed to the appropriate fund type. These efforts will be coordinated with and reviewed by the Office of Financial Analysis on a regular and/or as needed basis.
- Separation of Financial Transaction Duties - There are several instances where assignments of duties or system access authority provide the opportunity for one individual to perform a complete financial transaction:
    - Billing - Three individuals have access authority to edit price list content, input billing, and upload billing data to the M-Pathways system. This access authority should be separated to ensure that no one person can modify prices and issue billings to the M-Pathways system. The BRCF does not have formal change management procedures to control changes to the billing system databases. These databases are prepopulated and extended prices automatically fill in when the service code and number of services is input as part of the billing process.

**Management Plan** - The BRCF Director will meet with all core facility directors and initiate a detailed review of current billing processes and existing controls. Gaps, risks, and liabilities will be assessed and specific plans to address each will be designed and

implemented. System access authority and business processes will be modified to ensure that no single individual can modify prices and upload billing data.

- Procurement - One individual initiates non-PO vouchers for up to \$5,000 without department approval, reconciles the Statements of Activity (SOA) to source documents, and provides a spreadsheet summarization of the SOAs to the BRCF Director. The Director reviews the spreadsheet and matches totals to the SOA without a detailed item by item review of the SOA. Funds could be expended for inappropriate purposes and not be promptly detected.

**Management Plan** - The Director of the BRCF will begin immediately to implement random, detailed examination of line items in SOAs that includes tracing samples of transactions to source documents. This policy and process will be included as part of written Standard Operating Procedures (SOPs) to be developed for BRCF central business operations.

In addition, as a result of this specific finding, the Director of the BRCF will expand this action plan to review all of the core laboratory procurement processes to assess responsibilities, signature authorities, review, and control processes. Any additional gaps that are identified that have the potential to allow for inappropriate use of funds will be corrected and changes will be documented in BRCF SOPs.

- Payroll - One staff member submits paperwork to the payroll department for temporary employees, receives and inputs timesheet data to the M-Pathways payroll system, and reconciles the Gross Pay Register to the Statements of Activity. This assignment of responsibility provides opportunity for one person to have complete control over adding a new temporary employee, submitting timesheets, and reconciling pay received in their name.

Supervisor approved time reports are returned to individual employees instead of directly forwarding the approved time reports to the departmental timekeeper. Undetected modification could be made to the timesheet after supervisory approval. Submission of approved time reports should be managed by approvers.

**Management Plan** - Temporary employee hiring requests will be initiated by the directors of the core laboratory in which the employee will be working. The paperwork will be completed by the BRCF Administrative Assistant and reviewed by the Director of the BRCF.

- Once the Director of the BRCF has provided signature authority, the paperwork will be returned to the appropriate Core Director who will provide the hiring paperwork to the appropriate Human Resources office for processing.
  - Employees no longer have access to their payroll time report after it has been signature authorized by their supervisor.
- DNA Sequencing Services and Billing Services - The DNA Sequencing Facility processes service and billing transactions through a comprehensive proprietary system developed by the Director. The system provides support to almost every aspect of the process. There are opportunities for improving the DNA Sequencing Facility's proprietary service tracking and billing application documentation, backup, recovery and business continuity, and security.
    - Application documentation requires updating.
    - Backup copies of service and billing data are maintained onsite in the Director's desk. There is no offsite storage.



- A complete restore of key application software and data, is not performed at routine intervals.
- The Director is the only person who performs billing. The staff person who has been given documented operating procedures as billing backup has never performed the billing function as part of backup training.
- The server that houses DNA Core test results and billing data is housed in an open tower in the main lab area. Doors are left open to the lab during the day and on first audit review of the tower, the mesh doors of the tower were unlocked.

**Management Plan** - DNA Sequencing management is addressing recommendations with the following actions:

- Updating online application documentation, to be completed by the end of December 2007. Upon completion, these documents will be printed out and kept in a binder, for offline references.
  - Developing offsite data storage as part of current efforts toward major Core expansion by:
    - Moving the server to a separate, secure location.
    - Keeping one set of backup tapes at the current location, this becomes the second data site.
    - Potentially transferring electronic backup copies of all data to another off-campus site where another level of backup to tape will be housed in a secure contracted data warehouse. DNA Sequencing management is consulting with Medical School Information Systems, Bioinformatics, and the scientific equipment vendor to obtain information for formulating a plan. The DNA Sequencing Director's objective is to develop a plan and determine a timeframe for implementing offsite storage during the fiscal year 2008 third quarter.
    - Identifying critical data structures, databases and web sites and planning to perform semiannual restores of those elements in October and April. All other components can be rebuilt from off-the-shelf software and hardware.
    - As of October 2007, the staff person assigned as billing backup received hands-on experience by performing the September internal services billing and will perform the monthly billing on a semiannually basis going forward. The staff person has also participated in the September external services billing and will do so on an annual basis.
    - The server doors have been locked, and will remain so while the server is in the lab. A review of alternative locations is underway, as described above. No timetable has been set, due to the complexity of the move.
- BRCF Policy and Procedure - There are no written policies and procedures for BRCF administrative processes including recharge billing and budget management. BRCF management relies on the experience and cumulative knowledge of long-term individual staff members. Documented policy and procedures provide a structure to business processes that serve as a standard and support in the event that unexpected changes in personnel occur.

**Management Plan** - The Director of the BRCF, working with the Administrative Assistant Senior will initiate the following plans:

- Review and inventory all procedures related to procurement, payroll, and billing so that a comprehensive list of processes requiring Standard Operating Procedures (SOPs) can be created. Once created, these SOPs will be maintained both as readily accessible e-files as well as a hard copy in a binder in the central office for access as needed by appropriate personnel.

- Prioritize these processes and create SOPs for the most critical processes first. Once completed, create a process for monitoring and updating in a timely manner when business processes change. Consistent and clear use of file names with version control will be a significant part of the overall process.
- Inventory complex spreadsheets and sophisticated billing/reporting database tools used for reconciling accounts, billing for services, monitoring revenue and expenses, and preparing annual budgets. Document their functions and operating procedures.
- Seek the assistance of a qualified systems analyst to review the current processes and systems used for central business operations with a specific aim of identifying redundant processes, and to identify and implement existing M-Pathways management reports where those reports will increase efficiency.

University Audits will conduct a follow-up review in the fourth quarter of fiscal year 2008 to assess progress on action plan implementation.

**University of Michigan Health System Professional Fee Services Patient Pay Collection Agency Review**

#2007-112-1

Issued October 26, 2007

A patient receives two separate bills for services received at the University of Michigan Hospitals and Health System, one for professional fees and one for hospital fees. Professional fees include those services provided by physicians, psychologists, nurse practitioners, social workers, and physician assistants. The Faculty Group Practice (FGP) manages billing and collection activities related to professional fee services. Hospital fees (facility) include supplies, laboratory tests, radiology, physical therapy, treatment rooms, room charges, and drugs. The University of Michigan Hospitals and Health Centers (UMHHC) manage the Hospital Financial Services Facility Billing and Collection staff that performs billing and collection activities for hospital fees. University Audits conducted a review of collection activities for the FGP and UMHHC. The focus of this report is the collection activities related to the FGP. The collection agency activities for UMHHC are discussed in a separate report.

The FGP uses external collection agencies for collecting over-due accounts for patient services. External collection agency activities begin when accounts have at least one balance older than 90 days from the bill date. Accounts are automatically transferred to pre-collection and collection agencies. Pre-collection is used prior to account delinquency and provides a friendly, early reminder that payment is now due or past due. Primary collection activities commence once an account is delinquent and secondary collections activities begin once an account is delinquent with no activity for more than one year.

**Control Issues:**

- **Patient Account Write-Off Approval** - University Audits tested write-offs of patient accounts for professional fee billing. A review of a sample of professional fee patient write-offs determined that collection documentation did not always provide justification or evidence of required management approval for the professional fee billing group to write-off an account.

Five out of twenty professional account adjustments reviewed lacked documented management approval for the write-off. The amounts written-off ranged from \$1,320 to \$29,869.

**Management Plan** - Effective August 6, 2007, staff must complete the write off approval E-form and send it to a supervisor or manager for approval if amount exceeds staff adjustment threshold of \$250. After approval is received, the staff member will make the adjustment in GE-IDX and note approval in invoice comments. An exception report will be reviewed monthly to ensure that write-offs exceeding established thresholds are approved by management. The Patient Financial



Services (PFS) Procedure Manual was updated and communicated to staff in August 2007. The professional fee billing group has revised adjustment guidelines for patient account write-offs as follows:

- \$0-\$250 Billing Staff can adjust, no further approval required
  - \$250-\$1,000 Patient Financial Supervisors and Assistant Billing Manager can adjust
  - >\$1,000 Billing Director can adjust
  - >\$1,000 Assistant Director Patient Financial Services (patient pay only)
- Collection Agency Fee Review - University Audits reviewed monthly invoices and payments for professional fee collection agency invoices and noted no formal process exists to review fees charged on collection agency invoices. A lack of a formal process to review and verify invoices could result in the overpayment of invoices. Though no formal processes exist, all payments sampled appeared to be appropriate and within contract terms.

**Management Plan** - PFS developed and implemented procedures to ensure the collection agency vouchers are reviewed and the commission is calculated accurately in accordance with agency contract.

- Policies and Procedures Documentation - Professional Fee Billing does not have written documentation describing some key business processes. Written policies and procedures are an integral part of a strong internal control framework and ensure continuity when there is employee turnover. Written policies and procedures should be in place to document activities, procedures, functions, responsibilities, and flow of information within a department to guide in the daily operations and activities.

The policies and procedures for the following processes should be developed:

- Data transfer and balancing
- Collection agency invoice review and payment
- Account write-offs

**Management Plan** - The processes identified have been documented in the PFS Procedure Manual and communicated to staff.

- Account Transfer Reconciliation - Professional Fee Billing electronically transmits accounts on a weekly basis to the collection agencies. A confirmation is received from the collection agencies to verify the data transmission was complete and accurate; however, this confirmation is not matched or reconciled with the outgoing data file. Reconciliations of data transfers ensure that transmissions are complete and that delinquent accounts are receiving appropriate follow-up. It is a key component of ensuring the integrity and security of protected electronic health information.

**Management Plan** - A procedure has been developed to reconcile the number collection agency claims transferred. This number is compared to a confirmation from collection agencies which include the dollar amount and number of the claims received by them via tape. The PFS Procedure Manual was updated and policy communicated to staff in August, 2007.

The internal control environment within the FGP Billing Office provides reasonable assurance that financial and operational processes for collection activities are appropriately executed. Improvements were recommended and implemented by PFS in approval and documentation of write-offs, review of collection agency fees, formal documentation of policies and procedures, and account transfer reconciliations. All issues have been appropriately addressed and no follow-up is required.

This audit is closed.

## FOLLOW-UP REPORTS

**Management of Employees with Close Personal Relationships – Business and Finance** #2007-810  
Original Report issued September 11, 2007 Follow-up Report issued November 8, 2007

We completed our follow-up to the audit of close personal relationships in Business & Finance. University Human Resources committed to distribute a communication to deans, directors, and department heads regarding close personal relationships including general procedures to establish and implement an approved management plan.

University Audits has reviewed the e-mail communication sent October 17, 2007, by University Human Resources to deans, directors and department heads. The e-mail clarifies requirements and provides useful tools to assist in the management of close personal relationships at the University.

This audit is closed.

**Dearborn Departmental System Administration – College of Engineering and Computer Science** #2007-308  
Original Report issued June 29, 2007 Follow-up Report issued November 9, 2007

University Audits recently conducted a follow-up review of actions taken by management to address the Information Technology issues in the original report. As part of this follow-up, University Audits asked Information Technology Services (ITS) at Dearborn to run a current scan of the CECS servers using eEye's Retina product to help identify server vulnerabilities.

The recent network scan revealed that many of the high risk vulnerabilities found by the scan performed during the original audit were successfully addressed by CECS management. CECS addressed these issues by shutting down unused servers and servers containing vulnerable operating systems, and applying security patches as necessary. CECS management successfully implemented corrective actions on the following application vulnerabilities discussed in the original audit report:

- Microsoft Graphics Rendering Engine
- Windows Messenger Service
- ASN.1 Code Execution Vulnerability
- Microsoft Server Service
- Windows Cumulative Patch Remote
- Windows Remote Procedure Call Cumulative Patch Remote
- Windows RPC / DCOM Interface

Along with the vulnerabilities discussed above, there were new high risk vulnerabilities identified by the scan. It is understandable that vulnerabilities show up in subsequent scans since new vulnerabilities are discovered every day. It is also not uncommon for existing vulnerabilities to be present on different servers. These new instances of existing vulnerabilities, in some cases, indicate servers that were not operating during the initial scan. Of greatest concern are high risk vulnerabilities that existed on the prior scan and are still open on the same servers. University Audits identified that CECS had not addressed the following application vulnerabilities discussed in our original report:

- Common Desktop Environment Subprocess Control Service
- SENDMAIL Race Condition
- Microsoft Windows Plug And Play
- Secure Socket Layer Vulnerabilities
- Microsoft Graphics Rendering Engine
- Windows Task Scheduler
- Null Session
- Microsoft Routing and Remote Access Service



CECS management is in the process of addressing these vulnerabilities. University Audits will perform another follow-up to ensure that these issues have been resolved.

In addition to those issues revealed by the original network scan, University Audits also made recommendations on other issues pertinent to sever administration within the College of Engineering and Computer Sciences (CECS). CECS Management is currently addressing these issues. These recommendations concern IT administrative processes including:

- Offsite Backups
- Administrator Documentation
- Administrator Training
- Risk Assessment Practices
- Policies and Procedures
- Incident Response Plan

The corrective actions proposed by management are continuing. In an effort to properly secure the CECS network environment, management needs to perform periodic scans and immediately address vulnerabilities which, if unaddressed, could have irreversible effects on sensitive information.

University Audits will continue to follow the progress of the open issues with a second follow-up during January 2008.

**Office of Technology Transfer- Key Processes**

#2007-105

Original Report issued November 28, 2006

Follow-up Report issued November 13, 2007

Office of Technology Transfer (OTT) management has taken appropriate corrective action on all three audit recommendations and all new procedures are documented.

Reconciliations: The office manager reconciles the Gross Pay Register to time reports on a monthly basis. The Statement of Activity is also reconciled monthly and procedures have been appropriately separated and documented. The financial specialist reconciles the financial data in TechTracS, OTT's internal system to M-Pathways.

Monitoring and Tracking of Accounts Receivable (AR): Financial license terms for existing licenses have been entered into TechTracS. Over \$750,000 in license term receivables have been invoiced to licensees since the audit. New license terms are entered into TechTracS at the time the license is entered into the system. TechTracS generates automatic e-mail reminders and invoices when payment is due. AR for license terms are tracked and monitored monthly. The systems manager discussed OTT's receivables with Financial Operations personnel. OTT is adequately managing and recording AR.

Assessing Royalty Reports/Payments from Licensees: To help assess royalty reports and payments, OTT sends a Self-Audit Checklist to licensees within one week of initiating a royalty license agreement. OTT documented a formal plan and criteria for selecting which licensees to audit. A plan is in place to select and audit one to three licensee(s) by March 2008.

This audit is closed.

**U-M Flint Urban Health and Wellness Center Audit Report Follow-up Review**

#2007-207

Original Report issued March 8, 2006

Follow-up Report issued November 30, 2007

Management has addressed organizational structure and support, sanctions screening, and clinical business operations. They are in the process of establishing periodic provider licensing and certification validation.

UHWC M-Pathways financial information and newly developed UHWC financial reports indicate a growing deficit balance for the clinic.

The following is a summary of audit follow-up observations:

**1. UHWC Organizational Structure and Support**

The University of Michigan Health System (UMHS) and UHWC have extended the original Memorandum of Understanding (MOU) to continue the relationship to December 21, 2008. On July 1, 2007, UHWC entered into an additional MOU for collaborating physician services from the University's Department of Emergency Medicine. UHWC established their Professional Advisory Committee which is meeting on a quarterly basis. The UMHS Compliance Office, Office of General Counsel, Ambulatory Care Services, University of Michigan Hospital (UMH) Nursing Administration, U-M Risk Management, and U-M Flint Financial Services and Budget are represented. **Issue closed.**

**2. Provider Licensing and Sanctions Screening**

Progress has been made toward establishing provider licensing and certifications validation. The UHWC Clinical Services management is working with UMH Nursing Administration to complete a formal credentialing and privileging process for validating nurse practitioner and physical therapist licensing, and certifications on a periodic basis. They have assembled supporting documentation, established a credentialing and privileging committee, and requested procedures guidance from the UMHS Compliance Office. The UMHS Human Resources Director verified that UHWC management has submitted information necessary to include their employees in periodic and systematic screening of employees for federal and state sanctions. **Issue closed.**

**3. Clinical Business Operations**

UHWC management has developed written procedures for business and financial operations, and updated job descriptions to assign responsibility for day-to-day business operations. The grants and budgets administrator obtained one-on-one training from U-M Flint Financial Services and Budget Office staff to assume clinic billing and receivables functions and is currently performing timely billing and receivables tracking. Clinic management has worked with the U-M Flint Financial Services and Budget Office to develop new financial tools for tracking profitability, productivity, service statistics, and outstanding receivables on a monthly basis. The UHWC Professional Advisory Committee received these reports in October and will continue to receive them on a quarterly basis. **Issue closed.**

**Additional Recommendations for On-going Improvement and Support:**

- UHWC Management and UHWC Professional Advisory Committee continued guidance and oversight to assure appropriate staff performance of day-to-day operations
- A policy gap analysis with UMHS to confirm there are policies and practices in place to address state and federal laws
- U-M Flint Administrative Management monitoring of UHWC financial health



**University Audits – University of Michigan**  
**Open Audits Follow-up Table**  
**November 30, 2007**

Audit Title	Report Date	Issues	Expected Completion
U-M Computing Environment Kerberos Passwords 2007-304	6/22/07	Completion of the upgrade of Kerberos; implementation of pre-authentication; patch tracking; controlling Keytabs; potential for duplicate identities	December 2007
UM-Dearborn College of Engineering and Computer Science Departmental System Administration 2007-308	6/29/07	Vulnerabilities based on the periodic scanning of CECS servers	First follow-up was completed <u>November 2007</u> Second follow-up January 2008
Digital Media Commons CTools 2007-301	6/29/07	Controlling administrator privileges; restricting persistence of login sessions; log review, controlling 'friend' accounts; updating and signing the C-Tools SLA and formalizing the upgrade process	December 2007
Michigan Administrative Information Services – eResearch	11/26/07	Network placement of production server; required application items	March 2008
Department of Neurology Sleep Disorders Center 2007-206	6/22/07	Security issues; financial controls; charge capture timeliness; and data maintenance and backup procedures	February 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	May 2008
Adult NeuroRehabilitation Business Processes 2007-820	8/24/07	Patient access controls; charge capture; medical record documentation timeliness	December 2007
U-M Physical Medicine and Rehabilitation Othotics and Prosthetics Center 2007-107	9/24/07	Charge capture and cash handling controls; quality assurance processes	March 2008
Hospitals and Health Centers Permanent Art 2007-827	9/26/07	Coordination of roles and responsibilities; inventory maintenance and security follow-up	March 2008
University of Michigan Health System – Hospital Collection Agencies 2007-112	10/10/07	Collection agency fee reviews; policies and procedures documentation; account transfer confirmations and reconciliations	March 2008
Medical School Biomedical Research Core Facilities Financial Internal Controls 2007-826	10/23/07	Recharge rates; capital equipment; separation of duties; procurement; payroll; DNA sequencing services and billing services; policies and procedures	June 2008

Michigan Public Media Phase II 2006-806	4/24/06	Documentation and implementation of internal control policies and procedures	First follow-up was completed <u>May 2007</u> Second follow-up January 2008
Intercollegiate Athletics Sports Camps 2006-410	7/28/06	Second follow-up scheduled to ensure operational improvements were successful for the summer camp season	First follow-up was completed <u>May 2007</u> Second follow-up December 2007
College of Engineering – Minority Engineering Program Office 2006-813	9/29/06	CoE and MEPO jointly developing and implementing a management plan	December 2007
Procurement Services Procurement Card Program 2007-115	2/5/07	Phase I - Utilize data mining tools and reduce transaction based monitoring; additional focus on training and accountability of P-Card approvers, provide guidelines for card issuance; utilize electronic resources. Phase II – annual monitoring of card activity by dept.	Phase I – December 2007 Phase II – March 2008
Recreational Sports Business Office Internal Controls Review 2007-813	2/20/07	IM Building procedures were reviewed; action plans to be implemented in all Recreation Services locations	December 2007
Plant Operations Zone Maintenance Purchasing Controls 2007-812	4/24/07	Purchasing. New methods for handling inventory receiving and tracking	December 2007
Institute for Social Research, Cash Receipts Process 2007-815	5/25/07	Improved cash, check and credit card receiving procedures; documentation of business office accounting procedures.	December 2007
Matthaei Botanical Gardens & Nichols Arboretum, Business Office Internal Control Review 2007-817	6/19/07	Phase I – cash handling, instructor payment, and credit card refund controls. Phase II - unnecessary sensitive data in files.	Phase I December 2007 Phase II January 2008
Office of the Provost and Executive VP for Academic Affairs Fiscal Responsibilities 2007-201	7/16/07	Lack of certain written Policies and Procedures; oversight controls related to academic administrative searches	December 2007
Intercollegiate Athletics Academic Support Services 2007-408	7/18/07	Student counseling practices; employment and payroll controls; staff training and development	January 2008
Ross School of Business Dean's Office Fiscal Responsibility 2007-821	7/20/07	Purchasing; financial monitoring of their merchandise store; formalizing authority delegation; Statement of Account and Gross Pay Register reconciliations; employee overtime	December 2007
College of Literature, Science, and the Arts Biological Station 2007-205	8/6/07	IT controls, physical security and business processes	January 2008



Intercollegiate Athletics NCAA Compliance – Student-Athlete Equipment and Apparel 2007-409	8/24/07	Record retention	June 2008
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	December 2007
Intercollegiate Athletics NCAA Team Travel 2007-412	10/10/07	Cash and Travel Expense Vouchers Controls	March 2008