

UNIVERSITY OF MICHIGAN
REGENTS COMMUNICATION

Item for Information

Received by the Regents
November 19, 2009

Subject: Report of University Internal Audits
July through September 2009

Background:

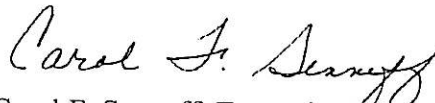
This is the report of the Office of University Audits activities for the period **July through September 2009**. The summaries of audits contained in this report were previously reported to members of the Regents' Finance, Audit and Investment Committee and included in discussions at Committee meetings.

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 **September 30, 2009**.

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

ORIGINAL REPORTS

Campus Audits

Deposit Process

#2009-103

Original Report issued on July 20, 2009

University Audits conducted a review of the cash deposit process for the University of Michigan. The Treasurer's Office has overall responsibility for the administration and oversight of all banking services for the University, including cash deposits. The Treasurer's Office has established a new process for cash depositing. Implementation of the new process began in 2006.

Process Outreach

Prior to the new process, the majority of units made deposits at one of the University's Cashier's Offices. Units had to submit hardcopy Cash Receipt Tickets (CRTs) with the deposit for each account (chartfield combination) where the deposit was allocated. The Cashier's Offices allocated funds based on these CRTs. Both the units and the Cashier's Offices counted cash, which resulted in unnecessary duplication of work. Some units had established bank accounts with a number of banks, thus creating a fragmented banking structure.

The majority of departments on the Ann Arbor campus, all the Cashier's Offices (Ann Arbor, University of Michigan Hospital and Health Centers (UMHHC), Dearborn, and Flint Cashier's Offices), and a few UMHHC departments converted to the new cash deposit process through a phased approach during 2006-2008. Individual departments on the Dearborn and Flint campuses and the majority of UMHHC departments did not convert and continue to make deposits through the respective Cashier's Offices. Units on the Ann Arbor campus still operating under the old process are those with infrequent deposit activity. The Treasurer's Office works with the Ann Arbor Cashier's Office to identify these units so conversion to the new process can be planned.

New Deposit Process Features

Every department that deposits via the new process is assigned a four-digit deposit location number and selects a default account. Employees with responsibility for cash deposits are required to attend deposit training after which they receive a depository certification. The Treasurer's Office policy requires recertification every two years. During the implementation phase of the new process, Treasury offered three-hour, instructor-led courses. Currently, training is offered via a more flexible, web-based eLearning course on MyLINC.

Some of the features of the new process are:

- The Treasurer's Office established a more consolidated banking structure for cash deposits. Bank of America is the University's primary bank for deposits. The Treasurer's Office has established alternative deposit accounts for a few exception units because of their business needs or geographical location.
- The new process resulted in a shift from departmental deposits at the Cashier's Offices to the bank. Cash deposits can be made in automated deposit stations on the Ann Arbor campus, at Bank of America branches, or they may be picked up for deposit by armored car or courier services.
- The general ledger is updated automatically with the deposit data from the bank.

- Departments that need to allocate a deposit across multiple accounts prepare an online CRT in Wolverine Access.
- Departments that allocate a deposit to a single account do not have to prepare a CRT.
- Cost of depository supplies, such as deposit bags and deposits slips, is absorbed by the Treasurer's Office.
- Each deposit unit uses deposit slips and endorsement stamps customized with their deposit location number.

Responsibilities

Several central departments at the University have responsibilities over the new process. The Treasurer's Office is responsible for establishing cash deposit-related policy and procedures, approving bank accounts, monitoring compliance with policies and procedures, and assisting departments with problems. The Treasurer's Office also provides training and education related to the new deposit process. Banking Services, a department within Financial Operations, is responsible for the bank statement reconciliation and assisting units with Statement of Activities (SOA) reconciliation. Transaction Services, another department within Financial Operations, is responsible for processing returned items. University of Michigan Administrative Information Services (MAIS) is responsible for setting up and maintaining an automated process to post deposit data sent from the bank to the general ledger on a daily basis. University units and departments are responsible for other controls, including segregation of duties related to cash deposits, proper deposit preparation, safeguarding of cash during the deposit process, and reconciliation of deposits to Statements of Activities.

The primary objective of this review was to assess the adequacy and effectiveness of controls related to the current cash deposit process. University Audits examined controls in the following areas:

- Physical security
- Training and education
- Deposits frequency
- Preparation of deposit
- Deposit data
- Bank reconciliation
- Returned checks

The following University units and departments were considered out of the scope of this review:

- Units that still utilize the old deposit process
- Units that make cash deposits through alternative, Treasury-approved bank accounts outside the new deposit process
- Individual departments and units that deposit cash through the Cashier's Offices. However, the Cashier's Offices themselves were within the review scope.

Control Issues:

- Monitoring - University Audits observed several areas where monitoring procedures can be improved. Specifically:
 - Not all University departments deposit cash in a timely manner as per Standard Practice Guide Section 519.03, *Cash Management Policies*. Five of the ten units tested are not making deposits in compliance with University and Treasury policies. Not making deposits in a timely manner increases the risk of theft and loss of funds and may negatively impact the University's cash management.
 - Bank errors (i.e., data entry errors) and unit errors (i.e., missing deposit slips) result in deposits not being allocated to the appropriate account. In cases of bank or unit errors, Banking Services investigates transactions and makes journal entries to reallocate funds

to the appropriate account. Some bank errors may stop the deposit journal file from posting to the general ledger, which requires investigation by Banking Services and journal file reload by MAIS. Errors result in additional work for the University. There are no formal procedures to track these errors. Without monitoring bank errors, management cannot accurately assess whether the bank is providing appropriate quality of service to the University. Without monitoring unit errors, Treasury may not have the information needed for targeted training and education efforts.

- The Treasurer's Office and Financial Operations do not monitor deposit adjustments made by the bank when discrepancies are found between the deposit slip and cash counted.
- University policy is not to accept foreign checks because of the high processing cost and delays in clearing these checks. The alternative is to accept other forms of payment such as wire transfers and credit cards. The bank does not accept foreign checks under \$100; these checks are returned to Banking Services. There are no formal procedures to monitor for foreign checks that go directly to the bank and are processed.

Management Plan

- SPG 519.03 Compliance - The Treasurer's Office recently filled a Senior Treasury Analyst position within the Cash Management Team. A Major Area of Responsibility for this position is to support the depository process. In the few months that this position has been filled, a number of new reports have been created that compile data on deposit activity, primarily from M-Pathways, but also from Bank of America's online reporting system. These reports have been extremely useful in preparing information to present to units during the Treasury Checkpoint Meetings that have been established during the last year. The purpose of these meetings is to meet personally with the major schools and colleges, and other depositing units to discuss their experiences with the new depository process and other services provided through the Treasurer's Office. During these meetings, a review a history of deposit activity for the unit is performed and any issues of non-compliance with the SPG policy are addressed. The initiative is to meet with the key administrators of these units on a recurring basis, preferably once per year.

This activity will cover the major depositing units, schools, and colleges; however, with the number of deposit locations now reaching near five-hundred, it is not feasible for the Treasurer's Office to monitor the activity of every depositing unit at close intervals with the current staffing levels. The data will be reviewed regularly, in aggregate, for use in maintaining the University cash flow forecast. These monitoring procedures will assist Treasury to identify units that are in non-compliance and address them on a case-by-case basis.

- Tracking of Bank Errors and/or Adjustments - This activity should be a collaborative effort between the Treasurer's Office and Financial Operations – Banking Services. Based on data provided by Banking Services, the Treasurer's Office compiles an accurate account of the number of bank errors and adjustments that occur monthly. It is the role of the Treasurer's Office to hold the bank accountable for making improvements to error rates as well as working with the depositing units and/or the bank to minimize the occurrence of debit/credit adjustments.

Currently, the Treasurer's Office meets with Bank of America monthly, including representation from Banking Services, to discuss and mitigate any new and/or outstanding depository issues. These meetings will continue going forward until a steady state is reached where all parties are comfortable.

Meetings with units concerning excessive depository errors will be handled case-by-case, as needed.

- Foreign Checks Deposits - With the recent bank merger, Bank of America can possibly offer the University the ability to post a “no foreign items” status on the depository account. If this is an available service for the University, any foreign items submitted for deposit would be rejected and returned, with a report generated by the bank that can be used for tracking. Further details for this service have recently been requested from the bank by the Treasury Manager and a response is being awaited.

If this service is not available, Treasury will again work with Banking Services to compile an accurate listing of any/all foreign items clearing through the depository account so the originating deposit unit can be identified and contacted to address the non-compliance issue. Once a monitoring process is in place, the Treasurer’s Office will document procedures and update the training materials if necessary.

- Automated Deposit Stations Security - The Treasurer's Office has installed four automated deposit stations on campus where departments can take deposit bags. Controls at these locations include surveillance cameras with live feed to the Department of Public Safety (DPS) and the Treasurer's Office and anti-theft alarm systems which alert DPS in case someone tries to break into the deposit station. University Audits observed the following control weaknesses:
 - The Treasurer's Office and DPS review the live feed or recorded video from security cameras only when needed (e.g., a department reports a problem with the deposit station, Treasury needs to verify a deposit was made, or DPS is investigating security issues). Lack of regular review may result in lost video footage due to obstructed or compromised view.
 - The deposit stations are not equipped with a panic button (a button an employee can press in an emergency situation that would notify DPS).
 - One deposit station is not equipped with an anti-theft alarm or live-feed camera.

Management Plan - The Treasurer’s Office will contact the manufacturer for the deposit stations to determine the feasibility of the recommended actions, considering equipment capabilities and cost implications. Where there is a reasonable business case to do so, these recommendations will be further explored for implementation. Where it is cost prohibitive to do so, or equipment limitations will not allow for such upgrades, the Treasurer’s Office will consider other alternatives.

The Treasurer’s Office will also establish a schedule to routinely check the status of surveillance monitors to ensure there are no obstructions to the camera view or malfunctions to the system otherwise.

- Treasurer's Office Procedures Documentation - Cash and checks deposited in the automated deposit stations are picked-up by an armored car company and delivered to the bank. The Treasurer's Office has documented policies and procedures for third-party deposit pick-ups in contractual language with vendors. Treasury has not documented procedures for situations such as missing or tampered deposit bags, unsealed deposit bags, or loose coins found in the deposit stations.

Management Plan - The Treasury Manager will document all procedures noted, providing copies to the Treasurer and those staff responsible for supporting the depository process.

The Treasurer's Office has developed a strong system of controls within the deposit process. Notable features include:

- Segregation of duties between central administrative areas (Treasurer's Office, Banking Services, Transaction Services, and MAIS)
- Robust training and education materials for department end-users
- Good communication between central areas to resolve problems in a proactive manner and to assist University units with questions and concerns particularly through timely response to a Treasury helpdesk email

University Audits will conduct a follow-up review in the second quarter of fiscal year 2010 to assess progress on action plans.

Intercollegiate Athletics NCAA Directed Review
Original Report issued July 24, 2009

#2009-401

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 assurances that existing procedures to monitor compliance are adequate. The Athletics Compliance Services Office (CSO) advised University Audits 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 agreed upon the goal of performing this directed review annually and to include all sports over a five-year cycle. Procedures include a review of select external camps and booster clubs to confirm an adequate system for tracking financial activity.

This review included the following:

Targeted Sports	External Camps	Booster Clubs
Football	Michigan Baseball Camp	U-M Club of Grand Rapids
Men's Basketball	Wolverine Distance Camp	U-M Club of Greater Chicago
Ice Hockey	Women's Gymnastics Camp	M-Women
Men's Gymnastics	Wolverine Swim Camp	
Women's Gymnastics	<i>(financial review only)</i>	
Women's Golf	Field Hockey	
Wrestling	<i>(compliance review only)</i>	

University Audits did not observe any areas of non-compliance with NCAA rules. Overall, the booster clubs reviewed have an adequate system for tracking and maintaining financial records. In general, the external camp revenues and expenses appear to be reasonable and related to camp operations. However, in some cases University Audits was unable to reconcile registration revenue records. A separate memorandum was shared with each camp director and Athletics management highlighting recommended business practice improvements.

DIRECTED REVIEW PROCEDURES

This section outlines detailed procedures performed for each compliance area. Unless specifically noted otherwise, procedures are for the 2008/2009 academic year.

Rules Education

- Reviewed CSO rules education packets for the coaches' meetings held during fall 2008 and winter 2009 to ensure coverage of key NCAA rules and regulations.
- Confirmed that the master schedule for rules education meetings include coaches, other Athletics staff members, other U-M non-Athletics department staff members, student-athletes, and representatives of the University's athletic interests.

Playing and Practice Seasons

For the targeted sports:

- Reviewed the practice logs for one week during the playing season for designated day off and weekly/daily hour limits for countable athletically related activities.
- Reviewed the practice logs for one week during the off-season for designated two days off and weekly hour limits for countable practice activities.
- Reviewed the declaration of playing season forms to verify compliance with first practice and competition dates, as well as the length of the playing season as applicable.

Auditor's Note: Compliance with NCAA regulations regarding limits on Countable Athletically Related Activities (CARA) could not be verified for the football team. Athletics requires coaches to submit their practice logs monthly. At the time of the review, which was after the 2008/2009 season, no logs had been submitted by football coaches. Football out-of season forms were submitted after the audit was completed and were therefore not reviewed by University Audits. Football regular season CARA forms still have not been submitted.

The practice logs help document compliance with NCAA mandated limits on countable athletically related activities. Athletics and CSO management are aware of this issue and are following up with the football program. A separate memo regarding this observation was issued to the Head Football Coach, the Director of Football Operations, and the Assistant Director of Football Operations.

Coaching Staff Limits

For the targeted sports:

- Confirmed the number of coaches in each category that were reported on the coaching staff lists is within NCAA limits.

Financial Aid

Individual Limits

For the entire student-athlete population:

- Verified that total financial aid and athletic-based financial aid reported in the University's system for the fall 2008 and winter 2009 terms was within NCAA limits.
- Confirmed the financial aid amounts in the University's system were not greater than the amounts actually reported to the Big Ten on the squad lists.

Team Limits

- Verified compliance with NCAA team limits for the targeted sports.

Eligibility

For the targeted sports (terms: fall 2008 and winter 2009):

Initial Eligibility

For a sample of student-athletes entering U-M during the 2008/2009 academic year:

- Verified initial eligibility report was obtained from the NCAA Eligibility Center and certification was completed within NCAA required timeframes.

- Confirmed enrollment in a full-time program leading to a degree.

Continuing Eligibility

For a sample of student-athletes who entered the U-M prior to fall 2008:

- Verified enrollment in a full-time program leading to a degree.
- Confirmed student-athletes were within the NCAA prescribed number of seasons of eligibility.
- Verified student-athletes had an Attestation of Eligibility form on file and met NCAA and Big Ten progress toward degree and minimum grade point average requirements.

Transfer Eligibility

For a sample of student-athletes who transferred to the U-M during the 2008/2009 academic year
(*Note: The targeted sports did not have any transfers, therefore sample was selected from the entire population of transfers during the 2008/2009 academic year*)

- Reviewed transcripts and other supporting documentation for a sample of transfer student-athletes to confirm the eligibility determination, including the one-year residency requirement, where applicable.

Camps

For selected camps, 2008 camp sessions:

- Reviewed compensation documentation submitted to Athletics to confirm that compensation for coaches and student-athletes is reasonably consistent with other counselors of like teaching ability and camp experience.
- Confirmed that free or reduced admissions were recorded on appropriate CSO forms and compliant with NCAA regulations.
- Reviewed bank statements and supporting documentation to ensure transactions are reasonable, have a clear business purpose, and appear to be related to the operation of the camp.
- Confirmed reasonableness of amounts reported on the Athletics Financial Disclosure form, based on documentation provided.

Boosters

For selected booster clubs, fiscal year 2008:

- Reviewed bank statements and supporting documentation to ensure transactions are reasonable, have a clear business purpose, and appear to be related to the operation of the booster club.
- Confirmed the amounts reported on the Athletics Statement of Disclosure form, based on documentation provided.

Complimentary Tickets

For one football, men's basketball, and ice hockey game during 2008/2009 academic year:

- Selected a sample of complimentary tickets for guests of student-athletes, non-U-M coaches, and prospects. Reviewed supporting documentation to confirm:
 - Recipients were clearly identified and authorized on the pass list.
 - Number of complimentary tickets were within NCAA limits.
 - Complimentary admissions were supported by properly executed documentation.

For one 2008/2009 men's basketball post-season game:

- Selected a sample of complimentary tickets for guests of student-athletes. Reviewed supporting documentation to confirm compliance with regulations bulleted above.

Recruiting

For a sample of prospects selected from the lists of prospects that made an official visit for each of the targeted sports:

- Reviewed the coaches' logs to confirm that off-campus contacts and evaluations were made during the appropriate periods and did not exceed NCAA limits.
- Reviewed the official visit form and related expense receipts to confirm:
 - Official visit took place after the first day of classes of the prospect's senior year
 - Prospect's file contains academic documentation used by the CSO for granting prior approval of the visit
 - Visit lasted no longer than 48 hours
 - Lodging, meals, and entertainment were consistent with NCAA regulations

University Audits and the CSO are working to improve the process for monitoring recruiting telephone calls for compliance with NCAA limits by establishing a continuous monitoring procedure. The continuous monitoring project is not yet complete and not all cell phone data was available; therefore, the review was performed on a sample basis.

The following table provides a summary of the 2008 review of recruiting telephone calls compared to the 2009 review:

Year	# PSAs in Sample	# of Sports in Sample	Review Process	Data Included
2008 Review	16	7	Manual review of coaches' phone logs	Available logs from August 2007 – January 2008
2009 Review	74	23	Automated review of telephone bills using analytical software	October 2008 and April 2009 cell phone bills; office phone bills from September 2008 through April 2009

The new continuous monitoring process will provide for an automated review of the office and cell phone bills for all prospective student-athletes' (PSAs) telephone numbers provided by each of the sport administrative assistants. All the necessary data will be forwarded by the CSO to University Audits on a monthly basis starting in fiscal year 2010, where analytical software will be used to automatically generate potential exceptions. These potential exceptions will be forwarded to the CSO for further investigation.

SUMMARY

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 and staff limits, financial aid, eligibility, recruiting, sports camps, boosters, and complimentary tickets. Overall, the booster clubs reviewed have an adequate system for tracking and maintaining financial records. In general, the external camp revenues and expenses appear to be reasonable and related to camp operations; however, registration revenue records could not be reconciled in some cases. University Audits will meet with the CSO during the second quarter of fiscal year 2010 to discuss the directed review procedures for the next year.

The University of Michigan-Dearborn Early Childhood Education Center (ECEC) is a State of Michigan licensed education and childcare center for children from one year old to kindergarten-age. Parents of children enrolled at ECEC include University faculty, staff, students, or members of surrounding communities. As part of the UM-Dearborn School of Education, the ECEC provides teacher preparation and child study for University students enrolled in a variety of education courses. During the 2008/2009 academic year, the ECEC offered such opportunities for approximately 130 practicum students, and employed another 80 students as general staff. The ECEC is also a research site for child study and best practices in early childhood education and teacher education.

In September 2008, the center collaborated with Oakwood Health Systems to move both the ECEC and an Oakwood Center for Exceptional Families program into a larger, shared facility. Moving into this new facility has allowed the ECEC to open additional classrooms and increase enrollment. Licensed capacity is 131 children.

The UM-Dearborn/Oakwood Hospital Healthcare collaboration facilitates opportunities to maximize the health, education, and empowerment of children with and without disabilities and their families and to prepare a new generation of teachers who excel in educating children with and without disabilities in inclusive settings.

The ECEC is funded from a variety of sources, including tuition from enrolled children, University general fund appropriations, and grants. At the former facility, the center, one of approximately 10% nationally of childcare and education centers with this designation, was accredited through the National Association for the Education of Young Children (NAEYC). Accreditation at the new facility is underway.

The objective of this audit was to assess the ECEC's business processes and childcare operations for compliance with University policies and State of Michigan Department of Human Services (DHS) regulations. The following potential risk areas were considered:

- Licensing/Accreditation
- Cash management
- Childcare center regulations
- Employment records
- Purchasing
- Payroll/benefit management
- Financial management
- Grant management

Control Issues:

- Aged Accounts Receivables - EZCare, the database used by the ECEC to track, among other things, each family's current balance, does not provide the ability to easily monitor and report on aged receivables. The report comingles negative and positive balances owed, is not editable, offers no comments field to track collections actions, and does not have the ability to group debts based on their age. These flaws have made collecting past due balances a very difficult and time-consuming manual process. In the past, the ECEC worked with the University-contracted collections agency to expedite customer payment. The center was unaware that the Cashier's Office is now working with a new collections agency that could resume the responsibility of contacting customers to encourage payment.

The ECEC is in the process of replacing the EZCare database. Management should work with the new vendor to ensure the replacement database will allow for simple aging, identification, and reporting of aged accounts receivables. Policies should be established that outline collections actions (e.g., phone call at X days past due, letter at X days past due) and establish thresholds for reporting. Management should contact the Cashier's Office to determine the appropriate process to send accounts of a certain age to the new collections agency. Accounts receivable should be monitored at least monthly and reported to upper management on a regular basis. In the short term, management should develop a process that would allow better identification and tracking of aged accounts in the current report (e.g., download to excel).

Management Plan - Management located an aging report in the EZCare database that identifies only past due balances, and groups them based on age. This report will be used instead of the previous ledger summary report. Management will also contact the Cashier's Office to discuss the process for forwarding delinquent accounts to the new collections company. Collections policies will be established, approved by the director, and shared with parents.

- **Timeliness of Deposits** - The ECEC collects funds from a variety of sources, including childcare tuition payments, fundraising, and third party sources (e.g., Box Tops for Education). Funds are deposited on Fridays, regardless of the day of receipt. In the event of the deposit preparer's absence, funds are held an additional week until the following Friday. Some payments were held up to three weeks from the date of receipt. Standard Practice Guide Section 519.03, *Cash Management Policies*, requires all funds to be deposited on the day of receipt. Deposits may be made the following business day if daily deposit is impractical and the total deposit is less than \$500.

Customer payments received by check are not restrictively endorsed upon receipt. Checks are endorsed immediately prior to the deposit, which may be one to two weeks after the check was received.

Management Plan - Deposit procedures will be modified to require daily deposits. The Secretary Intermediate will be trained on deposit procedures in the Secretary Senior's absence.

All checks will be restrictively endorsed upon receipt. Office staff, including the Business Manager, will attend the training on cash handling when it is available.

- **Physical Security of Cash** - At its previous location, the ECEC used a safe to secure cash until the day of deposit. Since moving to its current location in September 2007, the cash box is stored nightly in a locked file cabinet. The keys for the file cabinet are in the Business Manager's unlocked desk. In addition, the Business Manager's office is not locked at night. This is of particular importance since the Business Manager's office is located in the communal space of the building.

Management Plan - ECEC staff immediately resumed use of the safe to secure cash until a deposit is made. Employees were notified to resume locking their offices nightly. On subsequent visits University Audits verified cash was properly secured. **This issue is closed.**

- **Gross Pay Register and Statement of Activities Reconciliation and Review** - At the ECEC, the Business Manager approves timesheets, enters them into the system, and performs the review and reconciliation of the Gross Pay Register (GPR). No higher level review takes place. One individual should not be responsible for recording, approving, and reviewing payroll

transactions. SPG Section 518.01, *Payroll Controls*, suggests the following roles be separated to ensure adequate internal controls: approver, departmental timekeeper, and reconciler/approver. A higher level review can supplement controls when proper segregation of duties is impractical.

SPG Section 500.01, *Fiscal Responsibilities*, states financial controls are strengthened when separation of duties exist, ensuring one individual does not control a transaction from start to finish. At the ECEC, the Business Manager has purchasing authority and also reconciles the Statement of Activity (SOA) reports. There is no higher administrative review performed. In addition, the Business Manager does not sign and date the SOA reports as evidence of review.

Management Plan - The ECEC director (or the Education Coordinator, in the director's absence) will perform the final review of the GPR and the SOA. Each reviewer will sign and date the reports.

Auditor's Comment: The ECEC is transitioning to eReconciliation during Fall of 2009. eReconciliation is an online process to verify department financial transactions, versus the current paper process using the SOA report. This process will use online digital signatures and timestamps to identify the reconciler.

- **Customer Payment Receipts** - Customers have the option of paying at the ECEC via cash or check. Customers paying by cash are immediately given a receipt from a pre-numbered receipt log. Customers paying by check are told a receipt will be mailed when the payment is applied in the EZCare database. Due to the delay in payment processing, this may be up to three weeks after payment was made.

The current receipt log has an indicator for payment type, which includes check as an option. Office staff should utilize this feature to provide immediate receipts to customers paying by check. This method eliminates the need to mail check receipts, saving the ECEC associated printing and postage fees.

Management Plan - ECEC staff will provide an immediate receipt for customers that make a payment by check.

- **Documenting Hosting Events** - The ECEC does not use the P-Card Hosting Documentation form to provide details of hosting events. SPG Section 501.04, *Travel and Business Hosting Expense Policies and Procedures*, requires the P-Card Hosting Documentation form to document the purpose of the event, service of alcohol, if any, and list of attendees (where appropriate). This form allows reviewers to validate the business purpose and reasonableness of expenses.

In addition, hosting expenses on the P-Card statement are often classified as groceries or refreshments. Classifying these expenses specifically as hosting expenses allows the University to readily identify them. Certain internal controls in Accounts Payable, such as manual review of statements with hosting expenses, are dependent upon proper classification. Using incorrect classifications circumvents these controls and lessens their impact.

Management Plan - The ECEC will use the P-Card Hosting Documentation form following all hosting events. The Education Coordinator will review all P-Card Hosting Documentation forms for each event. Items purchased for hosting events will be classified as hosting expenses on the P-Card statement.

- Voucher Review - The current review process of travel expense forms and P-Card statements did not identify instances of incomplete or inaccurate documentation. Receipts for expenses often did not match the actual charged amount. A travel expense form was missing meal receipts, which are required by the center's reimbursement policy. In addition, The Business Manager updates information on travel expense forms based on information given by the traveler, but there are no notes to document these alterations. For example, one traveler submitted a reimbursement request for \$20.59, but the accompanying receipt was for only \$8.22.

Management Plan - Until October 15, 2009, when the new travel and hosting SPG is implemented, all missing receipts will be authorized by the Education Coordinator. When the new SPG is implemented, management will ensure compliance with the new travel per diem policy. At all times, any alterations to travel expense forms will be clearly noted. P-card expenses will have supporting documentation.

- Privacy of Employee Records - Employee background information, including FBI, Internet Criminal History Access Tool (ICHAT), Michigan, and DHS screening results are stored in labeled binders in an area accessible to all staff members and building occupants (including non-ECEC employees). These files include documentation related to offenses that may appear on an employee's background check, as well as medical health statements. Some records also include copies of an employee's driver's license or social security card. These documents are extremely sensitive in nature and should be secured away from common areas.

Management Plan - As an immediate fix, the area where documents are currently held will be locked nightly and when office staff members are not at the front desk. By October 2009, management will either use an existing locking cabinet or purchase a new locking cabinet, if necessary, to secure the documents. The key will only be accessible to the Education Coordinator or the Business Manager.

- Double-time Policy Issue - ECEC pays double-time for time worked between 7:30 a.m. to 8:00 a.m., and 5:00 p.m. to 5:30 p.m. This is done by increasing the total amount of hours payable to that employee, rather than coding the hours as double-time pay. The additions are done manually on each employee's timesheet by the timekeeper. The Fair Labor Standards Act and SPG Section 518.01, *Payroll Controls*, requires employers to keep accurate records of hours worked. SPG Section 518.01 also requires management to use the appropriate time reporting code for employee hours worked.

University Audits noted the following:

- The double-time pay agreement is not documented. Temporary changes to the agreement are also not documented.
- Several employees were either not paid the time when they should have been, or compensated when they should not have been.

Management Plan - A formal policy will be written that outlines the double pay policy. The School of Education Dean and the ECEC Director will sign the policy, and Human Resources approval will also be obtained. The updated policy will be distributed to all student staff. The Business Manager contacted a Payroll representative and determined a cash adjustment would be the most appropriate method to provide the extra pay.

- IT Security - The Secretary Senior's Windows login password is shared among student employees who work at the front desk. This is done to obtain access to various office forms

(e.g., sign-in sheets, permission slips) that are located on a network drive. An IT employee told the center he could not give student staff access to the network drives, so a decision was made to share a password instead. These student employees do have their own network login credentials. Password sharing is against UM-Dearborn's *Policy and Conditions of Use of ITS Computing Environments*, as well as general IT security best practices.

There are five desktop computers located in the communal lobby area- two at the front desk, one in the conference room, and two in a teacher work room located directly off the main lobby. The computers are not physically secured to prevent theft. There are no cameras in the lobby area, eliminating the opportunity to monitor the area. In addition, a computer in the conference room was observed logged in without screensaver password security.

Management Plan - ECEC has coordinated with UM-Dearborn IT personnel to arrange network access for the student employees. Office staff members now use their own account information to access the network drives. An exit/termination checklist will be used to ensure the network access is properly removed.

Computer locks will be purchased through IT and installed. Screensaver passwords will be added to all machines as a default once they are upgraded in October 2009.

Based on the audit work completed, the internal control environment at the Early Childhood Education Center provides reasonable assurance of compliance with University policies and State of Michigan Department of Human Services regulations for the operations of a childcare center.

A formal follow-up to the outstanding issues will be conducted in the third quarter of fiscal year 2010.

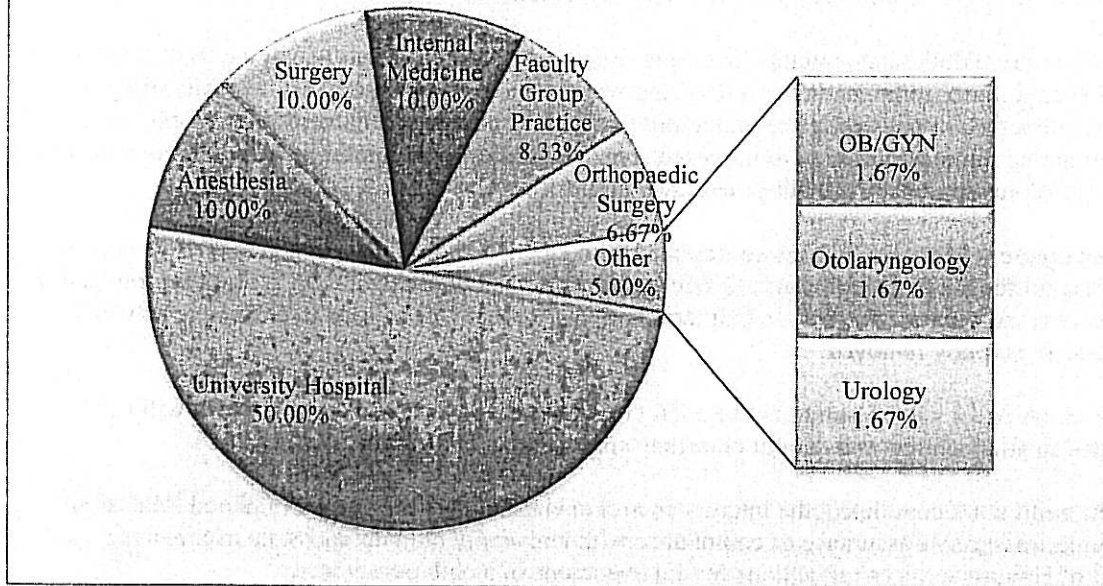
Health System Audits

U-M Hospitals and Health Centers East Ann Arbor Ambulatory Surgery and Medical Procedures Center
Original Report issued July 28, 2009 #2009-208

The University of Michigan Hospitals and Health Centers (UMHHC) East Ann Arbor Ambulatory Surgery and Medical Procedures Center (Center) opened in 2006. The Center has six outpatient surgical rooms, four medical procedures suites, and related support areas. This Center, which performs more than 6,000 surgical cases and 8,000 medical procedures per year, was created to ease increasing demands for outpatient surgical services and medical procedures on the University of Michigan (U-M) medical campus. It generates approximately \$60 million in annual gross charges.

The Center, which is governed by an executive committee (i.e., investors) made up of UMHHC and certain Medical School departments, is centrally managed by an administrative staff that reports to two medical directors. Profits are distributed to invested departments according to the shares held. Invested departments and share information are shown below.

EAA Ambulatory Surgery and Medical Procedures Center Investors



The audit focused on processes associated with the operation of ambulatory surgical units and medical procedures suites to determine if established policies and procedures and the internal control structure are sufficient to safeguard University assets and comply with specific U-M, UMHHC, federal, and state guidelines.

Specific objectives included:

- Reviewing charge capture practices to determine if internal controls are sufficient to ensure charges for services, medications, and other supplies are timely, accurate, and complete
- Assessing payroll controls to determine if payroll data is properly approved, reported, and reviewed
- Reviewing and assessing the control environment over the management of supplies, pharmaceuticals, and equipment
- Reviewing purchasing practices to determine if they comply with U-M and UMHHC guidelines
- Reviewing controls governing travel expenses to determine if travel expenses support U-M business purposes and are appropriately documented, reviewed, and approved
- Assessing operational controls over credit card payments, budgeting and financial reporting, and privacy practices

Control Issues:

- Building Security - During a walkthrough of the facility, University Audits noted the following:
 - a. An external building entrance marked "Staff Only" and the loading dock are left unlocked during normal business hours.
 - b. The loading dock is used as a temporary, unsecured holding area for certain supplies and equipment.

- c. Unauthorized individuals can gain undetected entry into administrative offices, recovery units, the Soil Room, which contains biohazard waste, and other parts of the facility from these areas.

Securing loading docks and other non-public entrances is a necessary component in protecting staff and assets. Unlocked loading docks facilitate deliveries from U-M departments (i.e., Materiel Services, Laundry Services) and non U-M vendors (i.e., UPS); however, they leave the facility open to potential risks and vulnerabilities such as theft.

Management Plan - Management will open discussions with Security and Key and ID Offices to explore options for securing entrances. Past review has presented challenges with maintaining an exclusive staff list, given access required by surgeons and residents, as well as multiple vendors delivering to the dock area. The dock area is not currently configured with phone, doorbell, or desk area for Center staff monitoring.

- Payroll Practices - A review of payroll practices and sampling revealed the following.
 - a. Monthly Employees Time Reports

Three exempt employees are not required to complete monthly time reports. They report exception time directly to the timekeeper. Exception time is not approved by a person with direct knowledge of the hours worked. SPG (Standard Practice Guide) Section 518.01, *Payroll Controls*, states that regardless of the method used to collect time data, the data must be approved before hours are entered into the timekeeping system.
 - b. Payroll Errors and Inconsistencies

In February 2009, the Center's timekeeper began entering time reports for staff at Kellogg Eye Center (KEC). University Audits reviewed a sample of twenty time reports, three of which were prepared by KEC operating room (OR) personnel, to determine if time reports were properly completed, authorized, and entered into the timekeeping system.

 - Reported time data for three individuals was inconsistent with employee time reports.
 - One employee erroneously received overtime for missing a 15-minute paid break.
 - One KEC time report was not approved by the employee's supervisor; three reports were not signed by the employee.
 - Some employees reported paid time off using the non-existent time reporting code PTO instead of PTS/PTX to report scheduled paid time off or PTU/PTY to report unscheduled paid time off.
 - Some employees reported time worked (9A.M. – 5P.M.) as opposed to the number of hours worked (7.5 hours) without providing sufficient information to ascertain whether an unpaid lunch break should be subtracted from the time reported.
 - c. Payroll Review Procedures

Staff members reconcile approved time reports to Payable Time reports (available in M-Pathways) and monthly Gross Pay Registers (available in DataMart) to verify time data was correctly entered into the timekeeping system and accurately reflected on department expense reports. However, the procedures applied to reconcile time data failed to detect and correct the errors noted in the first bullet of section 2.b. above.
 - d. Payroll Correction Documentation

Staff members may report payroll corrections to the timekeeper in-person, via e-mail, or through other delivery methods. The timekeeper does not maintain e-mails and other

documents supporting corrections or obtain approval for revisions from the appropriate supervisor. Per SPG Section 518.01, hardcopy documents supporting time data must be properly reviewed, approved, and retained for seven fiscal years plus the current year.

Management Plan

- a. Effective June 2009, exempt employees began completing monthly time reports that are approved by the Medical Directors. Monthly employees have always informed Center Medical Directors and staff of time away from the Center, and maintained personal GroupWise calendars. A public calendar is also posted in the administrative suite for all administrative and management staff, indicating planned time off.
 - b. Effective June 2009, signatures are mandatory to complete payroll processing.
 - c. Standardization of time reporting, including implementation of OR staff time reports at Kellogg, is in process. Past practice, particularly for OR staff, was not consistent. Time reporting codes for MNA (nursing union) staff were revised in conjunction with the new contract and began to be implemented in January 2009. The Center is working with UH OR administration to standardize time reporting across all OR sites.
 - d. Suggestions will be evaluated and implemented in a standardized way across all units (per item c. in Control Recommendations above). Procedures for reconciling the Gross Pay Register will be expanded.
 - e. Effective June 2009, any changes to initially approved time reports will be documented, approved, and retained in the payroll period files.
- Financial Controls - A review of financial processes revealed:
 - Incomplete and Inaccurate P-Card Holder Profiles
P-Card approvers are responsible for reviewing and approving changes to cardholder profiles. During a review of cardholder profiles, University Audits noted that one P-Card approver listed in M-Pathways does not match the name of the individual currently approving P-Card statements and one P-Card does not have a designated approver.
 - Unsecured Credit Card Terminal
The Center maintains a credit card terminal on a counter in the lobby. Credit card terminals are accessible to employees who are not authorized to process transactions. A password or special code is not required to operate the machine. The terminal is not secured during off hours. Additionally, the credit card terminal does not appear to truncate credit card numbers. Whole credit card numbers appeared on the merchant's copy of the sales receipt and the Detail Report printed from the terminal. Truncating credit card numbers reduce the risk of fraudulent transactions.

Management Plan

- Management completed and submitted Maintenance Forms to update approvers for both P-Card holders.
- Staff now stores credit card terminal in a locked drawer in the reception area during non-business hours.
- A new terminal ordered from the Treasurer's Office in April recently arrived and will be installed soon. The new terminal will truncate credit card numbers.

NOTABLE PRACTICES

Center Administrative Office personnel have instituted best practices in charge capture and revenue enhancement. The Center's financial analyst regularly reviews monthly third party-payor reports obtained from UMHC Billing and Third Party Collection Office (Billing Office). The reports provide

detailed payment information by payor and patient. The financial analyst sorts the data by insurance company codes, compares percentages of claims paid to fee schedules or historical reimbursement rate information, and investigates payments that are significantly outside expected ranges. Each month, Administrative Office personnel give the Billing Office a list of claims that should be resubmitted to third-party payors. In fiscal year 2008, the Center recovered approximately \$150,000 in revenues by resubmitting claims to payors. This practice, which increased efficiency and a greater number of first time correct claims in the Billing Office, resulted in a recoverable amount of \$70,000 in fiscal year 2009.

University Audits will conduct a follow-up review during the third quarter of fiscal year 2010 to assess progress on action plans.

University of Michigan Health System Clinical Research Billing
Original Report issued September 30, 2009

#2009-402

The University of Michigan Health System (UMHS) is a major clinical research center. At any given time, there are approximately 3,400 active medical research studies involving human subjects. Many of these studies involve patients enrolled in clinical trials, who receive both trial-related and other health care services at UMHS. Health insurance, federal regulations, and the intricacy of health care billing add complexity to billing related to patients enrolled in clinical research trials.

Clinical Research and Medicare

For eligible beneficiaries, Medicare covers routine patient care costs of clinical trials, as well as reasonable and necessary services used to diagnose and treat complications arising from participation in clinical trials. Routine patient care costs include all services that are otherwise generally available to Medicare beneficiaries. Medicare does not cover the procedure, device, or drug under investigation, nor does it pay for data collection and analysis. In general, UMHS follows Medicare clinical trial principles for other insurance carriers.

Clinical Research Billing Cycle

This is a high-level overview and does not reflect the detailed complexity of the process.

TERMS

DRDA – Division of Research Development and Administration assists in development of externally funded research projects. They approve all grant applications and conduct sponsor negotiations.

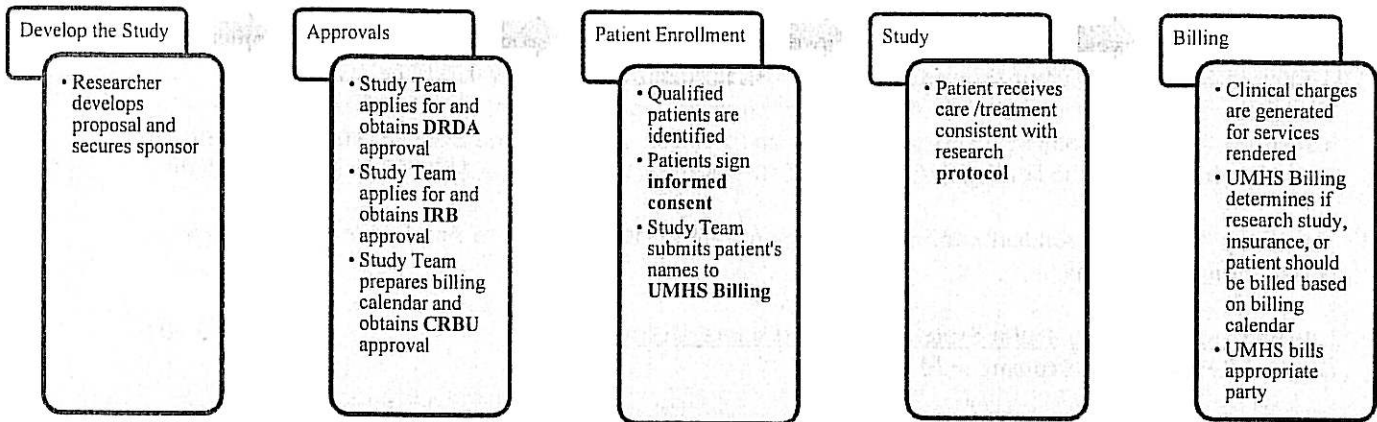
IRB – The Internal Review Board protects the rights and welfare of participants in clinical trials and other research involving human subjects.

CRBU – Clinical Research Billing Unit ensures a billing calendar is created and that study documents align and are consistent with federal regulations.

Informed Consent – An informed consent document contains specific, required information about the study. It is the formal patient authorization to participate in the proposed clinical research.

UMHS Billing – Professional Fee Billing and UMHHC Billing and Third Party Collections are the billing operations for UMHS.

Protocol – A research protocol is the plan for a course of treatment. It is reviewed and approved by the IRB.



Billing Calendars

As part of quality assurance, CRBU ensures that all study documents (protocol, consent, budgets, contracts/grants, billing information, etc.) align and do not conflict with federal or University research billing policies. CRBU also reviews and approves billing calendars. A billing calendar is a core compliance tool used collaboratively by the study teams, CRBU, and UMHS Billing to track research-related versus routine patient care services. The calendar is used to facilitate billing.

Process Review and Control Assessment Summary

University Audits performed a process review and control assessment of the clinical research billing process. Significant process development activities are underway. UMHS management has initiated:

- A dedicated resource of experienced personnel to advise and assist research teams in completion of billing calendars
- Coordination between research teams and UMHS Billing
- A Medical School process improvement steering committee, made up of clinical research faculty, research administrators, billing administrators, and legal counsel. The steering committee supervises the process improvement progress and has been instrumental in seeking a streamlined, compliant process.

Despite progress, risks and inefficiencies remain:

- There is substantial rework and rebilling due to a lack of a fully integrated process
- There is significant billing calendar backlog
- Coordination and communication between individual research units is not always effective resulting in a fragmented and incomplete process.

Based on our review and analysis, University Audits recommends additional opportunities for improvement which are outlined below.

Opportunities for Improvement

1. Leadership

There are multiple units across the health system and University campus that contribute to the clinical research billing process. These units include Division of Research Development and Administration, Institutional Review Boards, Sponsored Programs, the Medical School, individual researchers and research units, and the University of Michigan Health System. University Audits recommends the appointment of one or two executive champions to facilitate

integration with other research enterprise executives. Responsibilities should include developing both strategic and tactical plans to streamline research and business processes.

2. Research Planning

Robust coordination and planning are needed to improve the clinical research billing process. Research grant budget negotiations and human subject protocol development have a downstream impact on clinical research billing. Clinical research billing needs to be integrated with DRDA's grant proposal process and the IRB's human subject approval process to ensure a compliant and efficient process.

3. Integrated Solutions

The current clinical research billing process relies heavily on manual, labor intensive processes. An integrated electronic system is needed for clinical trial budgeting, enrollment, and billing calendar creation. UMHS Management is currently evaluating comprehensive software solutions. Near-term and longer-term solutions are required. The following should be considered early in the implementation:

- a. Development of a detailed project plan with key dates and milestones
- b. Inclusion of key process owners (DRDA, IRB, research community, Medical School, CRBU, and UMHS Billing)
- c. Dedicated implementation staffing
- d. Dedicated training for researchers and study teams

4. Interim Solutions

Implementation of an integrated electronic system will take time. In the interim the current process needs improvement to address risk areas:

- a. Define and Prioritize Back Log - Ideally, research involving clinical trials can take several months to years before patients participate in the clinical phase of a research trial. As a result, the CRBU has a substantial number of billing calendars that are in various stages of processing. University Audits developed several tools in their analysis that can be used by the CRBU on an on-going basis to identify which clinical trials have research subjects and are more likely to need priority billing calendar completion.
- b. Management Reporting - The CRBU does not currently provide standardized reporting to management. Basic monitoring reports will assist management in developing more robust reporting tools in the electronic system. Consider establishing production goals and developing key metrics for management to review on a monthly basis. Metrics are essential in monitoring compliance. Example statistics include but are not limited to description and quantification of backlog, billing calendar completion statistics, number of enrollees, and dollar volume of research billings.
- c. Develop an Escalation Process - The CRBU has difficulty getting study teams to consistently respond to inquiries. An escalation process is needed to help with non-responsive researchers. Consider engaging the Medical School's Office of Regulatory Affairs or other Medical School Administration to assist with the process.
- d. Communication with Research Teams - In the spring of 2007, there was a system-wide effort to train researchers and their study teams on the billing calendar process. Some training materials developed in 2007 are out of date and subsequent changes to the process have not been fully communicated to the research community. Consider updating training materials and conducting Town Hall style meetings to raise researcher awareness and understanding of their current responsibilities.

5. Policies and Procedures

There is currently no authoritative policy for clinical research billing. Policies and procedures are critical tools to ensure institutional regulatory compliance and to minimize staff confusion. Authoritative UMHS policy is needed that includes overall compliance requirements and incorporates an escalation process and sanctions.

Management Plan

Progress has been made on the issues amplified in this report. Plans are underway to integrate the CRBU into the clinical research trial activation process and to develop authoritative policies for clinical research billing.

1. Leadership

The Assistant Dean for Research will take executive leadership for this endeavor. He will report to the Senior Associate Dean for Research and the Senior Associate Dean for Clinical Affairs. A standardized report will be developed to regularly inform UMHS leadership, particularly the Executive Vice President for Medical Affairs, Dean of the Medical School, and the Chief Executive Officer of the Hospitals and Health Centers.

2. Research Planning and Integrated Solutions

A Working Group is being formed and will include representation from DRDA, IRB, eResearch, UMHS Billing, Information Technology Services, and research administrators and investigators to appropriately integrate the Clinical Research Billing process into the overall clinical research infrastructure. Moreover, the CRBU is just beginning a formal Lean process improvement exercise, lead by a qualified Lean coach, to examine and streamline the internal processes of the CRBU and its interactions with research teams, the IRB, DRDA, and UMHS Billing. CRBU leadership has already instituted JIRA tracking, a project management software tracking package, to examine work flow, timeliness of the operations, re-work, and points of communication with the research teams and UMHS Billing. This data will be invaluable in the Lean exercise and to expedite overall process improvement.

A new manager for the CRBU, who has extensive experience in billing unit management and medical coding, began September 1, 2009. Major unit goals under the manager's responsibility include implementation of rapid turnaround in the analysis of the billing calendar with feedback to the research teams and assumption of responsibility for the review of patient payment responsibility language in the Informed Consent. Concurrent with operational enhancements to the CRBU, UMHS management has evaluated comprehensive software solutions that will allow research teams to produce a standardized billing calendar, allow streamlined pricing of clinical items and services, and produce detailed budgets so that research teams can appropriately negotiate study payment from sponsors. UMHS Billing will use these standardized billing calendars to adjudicate charges to either third party insurance payors or research sponsors.

Inclusion of key process owners and dedicated training for research teams is integral to the roll-out of a comprehensive software solution. The Steering Committee and appropriate sub-committees for the software implementation are being formed. The Steering Committee, comprised of representative leadership from departments, billing, IT, and the Office of Research, will guide CRBU leadership in the construction of the project plan and establish key dates and milestones. It will also provide direct project oversight and advocate for the necessary resources to ensure successful and timely implementation.

3. Interim Solutions

- a. Define and Prioritize Back Log - The data provided by this audit has been used to prioritize and examine studies that are incomplete. The studies with active enrollment have been the unit's top priority for establishing resolution with the study teams. Many dated studies were found to be low-risk for billing concerns and have been retired. This systematic review of the audit results is a high-priority and should rapidly resolve our study back log.
- b. Management Reporting - The JIRA tracker is being used to analyze production concerns and establish productivity metrics and goals. Further refinement of the JIRA system currently underway will equip the CRBU leadership with a tool to provide standardized, real-time status reports on key metrics that will be used for operations improvement as well as keeping UMHS leadership informed of ongoing progress. CRBU leadership has established a routine and ongoing monitoring program with the UMHS Compliance Office.
- c. Develop an Escalation Process - The CRBU leadership has recommended that billing calendars be mandated, similar to other regulatory requirements, by no later than the first quarter of 2010. Similar to IRB approval, billing calendar approval should be required prior to allowing patient accrual on a study.
- d. Communication with Research Teams - Currently, CRBU staff is providing individualized, consultative services to study teams. A robust education program is necessary and will coincide with process enhancements and mandating billing calendars. A CRB training session has been integrated into the general clinical research training offered by the Michigan Institute for Clinical and Health Research (MICHHR). This general training will be augmented by Town Hall style in-depth training sessions. Online training is also being pursued. A mandatory module in M-Learning or Program for Education and Evaluation in Responsible Research and Scholarship certification is under consideration.

4. Policies and Procedures - Developing standard operating procedures and an authoritative institutional policy for clinical research billing are priorities of the unit and Office of Research leadership.

Auditor's Conclusion

Academic medical centers participating in clinical research continue to evolve integrating complex and diverse research activities. Each academic medical center has to develop processes best suited to their individual culture and structure. The Clinical Research Billing Unit and the UMHS Billing Office are progressing in the development of an effective and efficient billing process. A streamlined integrated system that includes key stakeholders will further ensure efficient and compliant clinical research billing. University Audits will perform a follow-up review in the fourth quarter of 2010.

University of Michigan Medical School Animal Research Process Controls
Original Report issued September 30, 2009

#2009-403

The care and use of animals is integral to the research and educational mission of the University of Michigan. The University of Michigan Policy Statement on Animal Research¹ states:

The University recognizes its legal and ethical responsibilities to ensure that animals are not used needlessly and are spared all unnecessary pain and distress. To this end, the University adheres to all applicable federal, state, local, and institutional laws or guidelines governing animal research, and has maintained since 1962 a University-wide Laboratory Animal Medicine Program directed by veterinarians specialized in laboratory animal medicine.

¹<http://www.vpcomm.umich.edu/pa/key/animal.html>

Oversight and management of animal use is administered by two key units, the University Committee on Use and Care of Animals (UCUCA) and the Unit for Laboratory Animal Medicine (ULAM).

UCUCA members are appointed by the Vice President for Research with documented delegation from the University President to advise, monitor, inspect, and oversee the University animal care and use program, facilities, and procedures. The committee consists of University faculty members and administrators and two community members that serve three-year rotating terms. The committee reports to the Office of the Vice President for Research (OVPR). Permission for any animal research at the University must be applied for through the development of an animal use protocol which is reviewed and approved by UCUCA. There are currently approximately 1,000 active animal research protocols and 500 principal investigators at the University.

ULAM provides veterinary and animal husbandry services and is part of the Medical School. All University animals are required to be under ULAM veterinary care and most animals receive ULAM husbandry services. A small percentage of University animal research projects provide their own husbandry services.

Regulatory Compliance

Three primary federal standards guide animal research and use at the University.

- National Research Council (NRC) *Guide for Care and Use of Laboratory Animals*
 - The NRC is an advisory and policy-making body under the auspices of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine.
- U.S. Department of Agriculture (USDA) *Animal Welfare Act*
 - The Animal and Plant Health Inspection Service of the USDA determines standards of humane care and treatment of animals under the act and monitors compliance through inspection.
- U.S. Public Health Service *Policy on Humane Care and Use of Laboratory Animals*
 - The Office of Laboratory Animal Welfare (OLAW), which is part of the National Institutes of Health (NIH), provides guidance and interpretation for this policy. All NIH-sponsored animal research is governed by this policy. Receipt of NIH funds and certain other federal grants require approval for animal research and assurance from the University to remain in good standing. The Vice President for Research is the institutional official and signatory of the assurance.

In addition to federal standards, the Association for Assessment and Accreditation of Laboratory Animal Care International (AAALAC) accredits the University's animal care and use program. AAALAC is a private, nonprofit organization that promotes the humane treatment of animals in science through voluntary accreditation and assessment programs.

University Audits Process Review

University Audits reviewed UCUCA and ULAM operational processes in cost accounting, purchasing, animal tracking, protocol management, and monitoring. University Audits noted internal controls and processes were well established for many aspects of animal care operations:

- Animal care cost accounting methodology is consistent with federal cost accounting principles.
- ULAM animal purchases are well documented and controlled.
- There is well-established monitoring of animal transfers and expiring research protocols.
- Substantial training is offered to research teams and animal care staff.
- Post-approval monitoring of research protocols was expanded in fiscal year 2009.

In addition, UCUCA and ULAM management are planning several process improvement initiatives:

- *Training* – Researchers are required to take as many as six training courses before participating in animal research. Currently these courses are offered in-person, lecture-style. In fall 2009, UCUCA and ULAM are moving all of its course registration and some of its courses to the University of Michigan Health System electronic learning system, MLearning. This will allow researchers greater flexibility in training and will provide better tracking of training requirements.
- *Information Systems* – UCUCA and ULAM currently use commercial software products called eSirius and Sirius for animal research protocol management and animal/husbandry management, respectively. These applications are stand-alone and not well integrated with other University systems. Information and Technology Services (ITS) recently received approval to develop an animal management component for the University's eResearch system, which will improve integration, data integrity, and reporting.

Opportunities to strengthen processes were identified during the review and shared with ULAM and UCUCA management. A summary of opportunities are listed below:

- Systematically link final approved grant activity to protocol monitoring.
- Increase monitoring, tracking, and reconciliation of animals purchased outside of ULAM.
- Improve coordination with the Sponsored Programs Office of Contract Administration to ensure UCUCA is notified promptly during contract negotiation of future subcontractor off-site animal use.
- Use an online registration system to more effectively track training requirements.

In fiscal year 2009, UCUCA introduced an enhanced post-approval monitoring program to ensure that principal investigators' activities conform to the terms of their protocols and to University policies and guidelines on animal care and use. The new program has received positive feedback from investigators and is well underway. Opportunities for improved post-approval monitoring were noted in standardizing documentation, reporting, and follow-up.

Conclusion

Animal research requires complex support systems that integrate research teams, federal regulators, granting agencies, and University business operations. Given this complexity, internal controls are in place for most animal management processes, but opportunities exist in several areas to improve operational efficiency and compliance.

Follow-up Reviews

Sponsored Programs Subrecipient Monitoring Follow-up Review

Original report issued on November 21, 2008

#2008-501

Follow-up report issued July 15, 2009

The Subrecipient Monitoring audit report outlined opportunities for improvement related to subrecipient monitoring guidelines, monitoring for Federal requirements, and addressing sensitive compliance areas. University Audits performed a follow-up review to determine the status of management's corrective actions.

Sponsored Programs and Contract Administration management has adequately addressed concerns raised during the audit. See summaries below for additional information. **This audit is closed.**

- Subrecipient Monitoring Guidelines - To help ensure subrecipient work is adequately monitored, management circulated an email to research administrators via the research administrators list serve, updated the subcontract cover letter sent to Principal Investigators (PI) for approval, and developed a comprehensive training course.

The email included a reminder that prior to approving payments, the PI is responsible for certifying that subrecipients are performing work consistent with the subcontract and sponsor requirements. It also emphasized that the PI should be signing the concurrence receipt sent with the invoice; department administrators should only sign if they have direct knowledge of the work performed or have received written assurance from the PI.

The subcontract cover letter was updated to include the following reminders for the PI:

- The PI should note any changes that need to be made to the subcontract, such as a more descriptive statement of work, reporting requirements, milestones, required deliverables, information regarding any potential patents, inventions or copyrights, or any cost-sharing requirements.
- The PI is responsible for monitoring the performance of the subcontractor, not only for appropriateness of expenditures, but also to ensure the work is performed in accordance with the terms of the subcontract before approving payments.

The subcontract training course will be piloted at the end of the summer 2009 and incorporated into Sponsored Programs' regular training schedule. The PowerPoint presentation for the training includes the following topics:

- Criteria that define a subcontract/hybrid purchase order
- New requirement that PI's certify, at the time of subcontract initiation, they reviewed the budgeted cost and price provided by the subcontractor and expenses appear to be necessary and reasonable
- Increased documentation requirements for specific budget categories if the prime award is a Federal Contract
- Requirement for the PI to disclose any potential conflicts of interest so it can be further assessed and managed
- Documented procedures for handling indirect costs between the subcontractors and the University
- Subcontractor payments will only be made after the invoice is approved by the PI
- Additional terms and conditions that may be specific to each unique sponsor including those related to human research subjects, animal research, export control, and cost and auditing standards
- Invoicing and payment criteria including the PI's approval requirement, the right to refuse to approve a payment if the work is not satisfactorily completed, and the importance of a detailed Subcontractor Statement of Work with clear expectations and deliverables

- Monitoring for Federal Requirements - Contract Administration now employs the Federal Audit Clearinghouse database of single audit reports as part of their annual process for obtaining A-133 reports to ensure compliance for subcontracted non-profit entities. Beginning in 2009, Contract Administration also requests that subcontractors not subject to A-133 audits provide University of Michigan with a copy of their most recent financial statement audit report. Documented procedures were updated to reflect these changes.
- Sensitive Compliance Areas - To raise PI and subcontractor awareness of key compliance areas, the "Assurances" article in the subcontract template was updated to specifically mention compliance with animal use, human subject, and export control regulations. The existing

template also includes an article that requires the subcontractor to have a written administrative process for identifying and managing conflicts of interest and reporting all conflicts to the University of Michigan. These topics are included in the subcontract training.

University Health Service (UHS) HIPAA IT Security Follow-up Review

#2008-309

Original report issued September 2, 2008

Follow-up report issued August 12, 2009

A follow-up review was conducted to assess the corrective actions taken. A discussion of the outstanding audit issues and corresponding corrective actions taken by management is presented below. Appropriate corrective actions have been taken on all audit recommendations. **This audit is now closed.**

- Outdated Practice Management System - The old practice management system, slated for replacement, could not encrypt stored electronic protected health information (ePHI), and only supported HIPAA-mandated integrity controls to a limited extent. UHS was to ensure that the new electronic health record (EHR) and practice management system (eClinicalWorks) provided these capabilities.

Management asserts that all HIPAA requirements will be met by either the new operating system or the EHR software. Specifically, Windows Server 2008 disk encryption will protect stored ePHI, and the HTTPS protocol used by eClinicalWorks will protect the integrity of ePHI in transit.

UHS remains in contract negotiation for eClinicalWorks, a fully integrated practice management and EHR system. To support this system, all user accounts, servers, and workstations are being migrated from Macintosh to Windows and Active Directory. The magnitude of these changes and their potential impact on users are significant. Planning and preparation for these infrastructure changes has taken longer than management anticipated, consequently delaying the purchase and implementation of the EHR software that will run using this infrastructure. EHR deployment is now targeted for the third quarter of fiscal year 2010.

- Verification of Intranet Access - Access to the UHS Intranet was not being reviewed during routine access reviews by managers. UHS IT Services (ITS) planned to include the appropriate UHS Intranet group memberships in the quarterly access reports sent to UHS managers beginning with the November reporting cycle.

ITS has revised the quarterly access reports to include UHS Intranet access, and incorporated the granting and removal of Intranet access into the standard user add/remove cycle. University Audits reviewed the new user access report to confirm the changes.

- Vulnerabilities in Intranet Tools Server - Security vulnerabilities were identified in the UHS Intranet tools server. ITS planned to replace this server with a backup server that was fully patched.

The Intranet Tools server was completely rebuilt by November 1, 2008. Extra time was required due to the complexities of upgrading all tools and utilities on the server. UHS now performs a monthly security scan on this server using tools recommended by IT Security Services (ITSS), and looks for updates on a weekly basis at minimum.

- Emergency Data Access Procedures - UHS Security Policy required emergency ePHI access procedures. ITS planned to work with UHS business owners of systems that house or process

ePHI to write specific emergency access procedures establishing who authorizes emergency access for each data asset or system, how authorizations are recorded, and how access changes are reconciled, reprocessed, or reversed once the emergency condition has ended.

Because of the complete revamping of all systems, emergency access procedures are still under construction. The framework is in place, but ITS will need to insert details as the disaster recovery procedures are formulated for new systems. University Audits will review the final procedures as part of a future audit of the UHS EHR system.

- Security Policy Improvements - UHS Security Policy required that systems be able to automatically disable accounts that are idle or that exceed a predetermined expiration date. The Security Policy did not address the patching of servers. ITS planned to update the Security Policy to permit periodic review of expired accounts rather than automatic disablement, and require the patching of servers.

UHS plans to make the recommended changes while crafting and updating policy governing the new Windows infrastructure and EHR system. Management accepts a small amount of risk until that time. As noted in the audit report, actual practices regarding the review of user accounts and patching of servers are strong mitigating factors. University Audits will review the final procedures as part of a future audit of the UHS EHR system.

School of Music, Theatre & Dance Fiscal Responsibilities Follow-up Review

#2008-815

Original report issued November 26, 2008

First follow-up report issued August 12, 2009

The audit report outlined opportunities to improve processes related to financial oversight and monitoring, procurement, imprest cash funds, delegation of authority, conflict of interest, payroll, and the summer youth program (MPulse). A follow-up review was conducted to assess the status of management's action plans.

University Audits will conduct a second follow-up review during the second quarter of fiscal year 2010. See summaries below for additional information.

CLOSED OBSERVATIONS:

- Procurement Observations - SMTD Management made several changes to strengthen controls over the procurement process and ensure practices are consistent with University guidelines. The Business Administrator's access to initiate purchasing transactions was deleted. Procurement guidelines are among the topics covered in SMTD's monthly meeting of financial and human resources staff from each reporting unit. SMTD is planning to invite someone from Procurement Services to speak at the group meeting in September.

SMTD Management met with Procurement Services in July 2009 to review an analysis of their spending and whether or not the appropriate methods were used. The document developed for this meeting outlines a few opportunities for improvement in the use of P-Cards and Non-PO vouchers. The Chief Administrative Officer now requires that all expenses in his area of responsibility be presented to him in advance. This includes most of the accounts; the rest are either faculty discretionary accounts or scholarship accounts. This process has not yet been documented.

From January 2009 to June 2009 there does not appear to be any P-Card transactions that were split to avoid the \$5000 transaction limit, using the same P-Card or using more than one P-Card.

- Conflict of Interest/Commitment Policy (COI/COC) - The staff conflict of interest/commitment policy is now properly approved and implemented. The policy and a link to the training tutorial were distributed to SMTD staff in July 2009. Staff is required to sign and return the disclosure form by August 15, 2009. This process will be completed annually as part of performance evaluations.
- Miscellaneous MPulse Observations - All MPulse credit card transactions are now processed online; therefore, many of the concerns identified in the audit report no longer apply. MPulse no longer has a credit card terminal. With the new process, the Camp Administrator does not process the credit card transactions, but does process refunds. The online system has built in controls that require a transaction number to process a refund and will not allow a refund to a different card than was used for the original purchase. The Business Administrator now reviews refund activity on annual basis, after the camp session. The camp procedures will be updated to reflect the new credit card processing steps.

The camp administrator no longer uses a travel advance for petty cash needs during operation of the camps and obtained an imprest cash fund from Accounts Payable.

IN-PROGRESS OBSERVATIONS:

- Financial Oversight and Monitoring - Significant progress has been made to improve financial oversight and monitoring at SMTD. Management re-mapped each budget line to a new reporting structure that allows for multi-level reporting capabilities using reports from the University's M-Pathways systems. SMTD converted to the new reporting structure in July 2009. Once the July transactions have closed, the Business Administrator will send each department head with responsibility for monitoring budgets a set of specific reports generated from M-Pathways on a monthly basis. The Business Administrator will continue to monitor all accounts at a high level.

The SMTD Human Resources/Financial group began monthly meetings in January 2009. Topics covered in these meetings seem appropriate to help ensure consistency across units and share best practices.

The Business Administrator identified which accounts represent the highest financial risk for the School and created a spreadsheet to track the Statement of Activity reconciliations for all SMTD accounts. The Business Administrator now runs a query at the end of the month to determine which accounts had activity. The tracking spreadsheet will be maintained on a shared drive; this way it can be updated by all persons with this responsibility to reflect the most recent information. The SMTD Human Resources/Financial group is working on documenting reconciliation procedures.

During the second follow-up, University Audits will review a sample of:

- Monthly reports used to compare budget to actual expenditures on a regular basis and documented explanations for significant variances.
 - Reconciled statements and the documented procedures for completing the reconciliations.
- Imprest Cash Fund Management - SMTD Management is working to improve management of their imprest cash funds. All funds have been updated to reflect the correct higher administrative authority. During the second follow-up, University Audits will review the documented procedures for performing reconciliations, the reconciliation template, and documentation to support regular reconciliations as well ensuring that surprise reconciliations are being performed.

- Payroll Observations - To initiate steps for ensuring time is reported accurately, the SMTD Human Resources/Financial group is working on creating a list of approvers and staff for whose payroll they are responsible. The group is also working on documenting proper time administration, authorization, and Gross Pay Register reconciliation procedures. Staff will be trained on these procedures once the documentation is completely developed. During the second follow-up, University Audits will review the list of staff and approvers, a sample reconciliation, and the documented procedures.

OPEN OBSERVATIONS:

- Documented Procedures - Key operational procedures have not yet been formally documented. The Administrative Assistant to the Chief Administrative Officer has been assigned the responsibility of documenting procedures. During the second follow-up University Audits will review progress on documenting procedures including procurement guidelines and approval thresholds and updated MPulse credit card processing procedures.
- Written Delegation of Authority - Signing authority that has been delegated by the Dean to various individuals has not yet been documented. University Audits will review the status of documenting signing authority delegated by the Dean during the second follow-up.

MAIS Degree Audits

Original report issued November 14, 2009

#2008-123

Follow-up report issued August 13, 2009

A follow-up review was recently conducted to determine if the corrective actions taken by management have adequately addressed the control issues raised during the audit. Details regarding action plan implementation are noted below. Appropriate corrective actions have been taken on all audit recommendations. **This audit is closed.**

- Academic Advising
 - The Office of the Registrar committed to consult with schools, colleges, and departments to identify ways to modify the Degree Audit Report to more closely reflect student transcripts. The Degree Audit Office's support of completed and on-going degree audit implementations in the Schools/Colleges has provided continuous opportunities to identify such improvements in business processes and reporting needs.
 - Monthly meetings are held with the College of Literature, Science, and the Arts (LSA) and the College of Engineering (CoE).
 - Meetings with other Schools/Colleges are held on an as needed basis.

The Degree Audit Office also plans to schedule annual meetings with the other Schools/Colleges, starting in the 2009-2010 academic year. These consultations with the Schools/Colleges will provide the Degree Audit Office with an understanding of the Schools/Colleges business processes and reporting needs.

- Calculating GPAs When Courses Are Repeated
 - Information and Technology Services (ITS, formerly MAIS) and the Office of the Registrar committed to working together to properly reflect client requirements for calculating GPAs when a course is repeated.
 - The Engineering Physics and Nuclear Engineering and Radiological Sciences departments in the College of Engineering have re-evaluated how their Major

GPA's are calculated. As a result, degree audit setup changes were made, eliminating the need for exception-based calculations when a course is repeated.

- Additional consultation is needed in other departments using such exception-based calculations. This consultation effort will be described at the next monthly meetings between Degree Audit and LSA and Degree Audit and the CoE.
- In the other Schools/Colleges, such exception-based calculations will be addressed at the annual meeting.

- Entering Exceptions

- ITS and the Office of the Registrar agreed to examine the process of entering exceptions to find ways to make it more user-friendly and to consider sending an email notification to a student when an exception has been entered.
- The Degree Audit Office and SRCAA (Student Records, Curriculum, and Academic Advising) Performance Support team are working together to develop an e-class, which will be followed by a one-on-one session, customized for each School/College's exceptions. This e-class will provide a user the flexibility of reviewing the data entry process on an ad-hoc basis, as often as needed.
- Although no action was taken, the Office of the Registrar and ITS looked at the possibility of streamlining the data entry of exceptions.
- Modification of the Degree Audit System to send email notification to a student upon data entry of an exception will be evaluated when the M-Pathways Student Administration notification system is implemented.

Research Computing at the College of Engineering

Original report issued October 29, 2008

#2008-302

First follow-up report issued September 3, 2009

A recent follow-up review examined open audit issues and corresponding corrective actions. Management has addressed many of the open issues through implementation of positive changes that will strengthen internal controls. Some issues are still being addressed; measurable progress is being made on all of these issues.

- Unsupported Devices - An unsupported device is defined as anything that uses the network and is not directly supported by information technology (IT) staff. In the CoE, this includes sensors, measuring devices, various laptops, and smart phones (i.e., Blackberry and iPhone). While these devices are not actively supported by CoE IT, they make active use of the network, and in some cases carry U-M data. University Audits recommended that CAEN and departmental IT groups create a best practices document to provide guidance for the users of unsupported devices. CAEN is working with CoE IT departments to develop a comprehensive document. **Work on this item continues.**
- Users with System Administrator Privileges - Security best practice dictates that users be given restricted accounts on their computers. This prevents the user from accidentally making critical changes, inadvertently installing malicious software, or making changes that could harm other systems on the network. Sometimes a user's needs create the necessity to give that user administrator-level privileges. University Audits recommended the implementation of a process to track which users are given administrator access and for what purpose. CAEN is developing documentation that CoE IT departments can use for tracking users with elevated privileges. **Work on this item continues.**

- Procedural Documentation - Throughout the CoE, IT groups have found creative and effective ways of handling a variety of problems. Good practices are in place for system configuration, incident handling, addressing vulnerabilities, and dealing with non-standard devices. Many of these solutions are not documented. University Audits recommended that each group review their current practices, procedures, and policies and ensure they are well-documented. CAEN is working with each IT department to create this documentation, and will be providing a repository for it in the form of a Wiki. **Work on this item continues.**
- Vulnerable Systems - University Audits used a system scanner to evaluate vulnerabilities on a sample of machines at selected departments within the CoE. The scans highlighted multiple systems with high-risk vulnerabilities. University Audits recommended that each department within CoE review the results of the scan for their area and eliminate vulnerabilities wherever possible. University Audits also recommended the implementation of comprehensive periodic scans to maintain a level of security on the network. CAEN has developed a scan process and ticketing system to identify vulnerabilities and notify appropriate administrators of their existence. The system automatically generates a ticket for each vulnerability detected. Tickets contain links to more detailed information and guidance on securing the vulnerability. **This item is now closed.**
- Unnecessary Services - Services are applications that allow a computer to interface with its components and the rest of the world. To carry out their functions, servers and workstations run a number of services. While some services like e-mail, web browsing, and hardware interfaces are necessary and appropriate; there are instances when computers run services that are neither. Scans revealed multiple unnecessary services running on multiple machines across the CoE. University Audits recommended CAEN work with departmental IT staff to identify potentially unnecessary services and disable them where appropriate. The scan process that CAEN has implemented will treat unnecessary services as vulnerabilities. Services will be identified and a ticket created. **This item is now closed.**
- Unknown Ports and Services - Services use ports as their means of communication. When a computer receives data, the data destination port on a machine helps the computer identify what service needs the data. A vulnerability scan found a number of computers with ports associated with unknown services running. University Audits recommended administrators close all unnecessary ports. Unknown ports are identified by the CAEN scans, and treated as vulnerabilities. Once ports have been discovered via the scan, CAEN staff work with system administrators to appropriately identify them so unnecessary ports can be closed. CAEN maintains a list of those ports deemed necessary, and the machines they are found on, so they may be closely monitored. **This item is now closed.**
- Unknown Systems - The networks within the CoE are kept open and are easy to connect to for the convenience of their users. Although this gives students and faculty a great deal of flexibility in addressing their computing needs, it also allows unknown, potentially non-standard, unsupported systems access to the network. These systems may not conform to the security standards of the department's IT group, and could cause harm to the network and the systems it hosts. University Audits recommended regular network scans to identify unknown machines. CAEN's scans identify all devices connected to the network. The list of machines scanned is compared to a list of registered machines. Any machine that is not registered is treated in the same manner as a vulnerability that has been discovered. A ticket is created and the school that owns the IP address in use is notified. Administrators can then appropriately handle the unregistered machine. **This item is now closed.**

- Updating Firewalls - Firewalls are essential to network security. They provide perimeter security, a barrier between machines on the network and the outside world, keeping the network more secure. Essentially, firewalls are just specialized computers. Like normal computers, they sometimes have vulnerabilities that need to be patched. University Audits recommended periodic checks of firewalls to ensure vulnerabilities are patched on a regular basis. CAEN is scanning firewalls along with all other systems on the network. Firewalls that have vulnerabilities will show up on the scans and be treated the same as any other system with a vulnerability. CAEN will also remind IT administrators of the importance of keeping firewalls up to date at their quarterly meetings with CoE IT departments. **This item is now closed.**
- Machine Setup - IT support groups at each department within the CoE perform nearly all of the new system builds and configurations. This provides for well-configured and secured machines being deployed to users. Currently, none of the IT support groups at selected departments within the CoE have their build or setup processes documented. University Audits recommended that each of these groups document their build process to ensure consistency. CAEN has developed, and made available, a fully configured version of Windows XP that school IT departments can install on their new systems. The “administrative load” is well-documented, and its documentation is available to all CoE IT administrators. CAEN has recommended to all CoE IT departments that the “administrative load” be utilized for new machines. If a department decides not to use the “administrative load,” CAEN has recommended that detailed documentation be created for the install based on the documentation for the “administrative load.” **This item is now closed.**

A second follow-up will be conducted during November 2009.

Michigan Administrative Information Services Grade System: Web-based Grade Changes #2008-113
Original report issued December 23, 2008 First follow-up report issued September 30, 2009

A recent follow-up review examined open audit issues and corresponding corrective actions.

- Role Assignment Guidance - User access within the Web-based Grade System is defined by roles. To maintain a highly flexible environment, role assignment is left to academic departments. This decentralized authority can create situations where roles are inappropriately defined and inconsistently assigned across campus. University Audits recommended that Information and Technology Services - Student Administration (ITS SA) work with Access Services (AS) to create documentation describing each role, the access associated with it, and recommended staff to be assigned the role. ITS SA is working with the Registrar’s Office to develop the documentation. This work is scheduled to be complete before Fall 2009 end of term grading.
- Customization Guidance - The Web-based Grades System provides academic units with a number of configurable options to help tailor the system to meet their needs. These options focus on user permissions, proxies, and automated notifications. This added flexibility can create situations where permissions and notification settings are adjusted by users in a manner rendering them inappropriate or ineffective. To reduce potential confusion over these options, University Audits recommended that ITS SA create documentation describing the customizable features, the impact of changes on security, and providing recommended settings for each feature. ITS SA is working with the Registrar’s Office to develop this documentation. This work is scheduled to be complete before Fall 2009 end of term grading.

- Two Factor Authentication Issue - The Web-based Grades System is accessed through Wolverine Access using a username and Kerberos password. Use of the MToken is not currently required. University Audits recommended that ITS improve security of the system by requiring use of the MToken for a second factor of authentication. ITS SA proposed this project. The project has been delayed due to budgetary concerns. While awaiting final approval, ITS SA is researching possible alternatives with a smaller budgetary impact.

A second follow up will be conducted during November 2009.

Active Directory UMROOT Domain Follow-up Review

Original report issued February 1, 2009

#2008-310

Follow-up report issued September 30, 2009

A follow-up review was conducted to assess the corrective actions taken. Appropriate corrective actions have been taken on all audit recommendations. **This audit is closed.**

The project to collapse the campus forest² to a single domain, eliminating the shared administration of the campus forest, is making progress. All groups have plans to complete their migration within fiscal year 2010. Housing has already completed their migration, and the Housing domain has been deleted. The College of Literature, Science, and the Arts and the College of Engineering are executing their plans for migration. Ross School of Business has met with LAN/NOS Groupware Services to review their plans.

- Exposed Telnet Services - Telnet services, which are used by the Exchange Servers to communicate with the storage area network (SAN), were open to the Internet. Data transmitted through Telnet is not encrypted and could be intercepted by eavesdroppers. The Windows team planned to move the service inside the UMROOT firewall once older Exchange Servers were retired.

Groupware Services has removed the older servers and repositioned the SAN behind the firewall with Telnet ports blocked. This was verified by attempting to connect from an off-campus location via the Internet using a Telnet client. No connection could be made to the Telnet services.

- Depth of Security Scans - Vulnerability scans of the UMROOT Windows infrastructure were limited in scope, covering only the top ten Windows vulnerabilities. Groupware Services planned to consult with ITSS, now Information and Infrastructure Assurance (IIA), to determine their options for obtaining more comprehensive security scans of UMROOT infrastructure.

IIA is doing more comprehensive security scans of the Active Directory infrastructure on a regular basis. Management has created a group to receive reports and assigned a staff member to review and act on detected vulnerabilities. Fine tuning of external scans continues, as does the development of procedures for responding to exposed vulnerabilities.

- Inactive User Accounts - User accounts in Active Directory (AD) were frequently not deactivated or deleted when the user left the University, resulting in a large number of inactive accounts. The AD user population is based on the U-M Online Directory (UMOD), which is being replaced by MCommunity. Management expected this replacement to provide more accurate user data, allowing more timely removal of AD user accounts. In the interim, they planned to document the

² Active Directory is a Microsoft system for locating, connecting, and managing Windows servers, workstations, applications, and users. It is arranged in the form of "forests" consisting of one or more domains.

criteria that MCommunity will use to determine whether a user should be granted AD access, and a plan for communicating the policy change to holders of excluded accounts.

Groupware Services has developed an automated mechanism for identifying inactive accounts, disabling them, and deleting them after a certain number of days. A dry run indicated 15,403 inactive accounts. Management has developed a communication plan and process. The identified inactive accounts will be disabled in October, followed by a regular monthly process to identify and disable newly inactive accounts. Broader limitations on community access to AD are contingent on MCommunity involvement, which Windows team management is still trying to secure.

- Incomplete Host Hardening - "Host hardening" (disabling unnecessary features and services) had been partially implemented within the UMROOT infrastructure. Management planned to apply the Security Configuration Wizard (SCW) to all UMROOT servers while upgrading them to Windows Server 2008. Servers scheduled late in the upgrade process would have the SCW applied separately in the interim. Management also planned to strengthen policy and monitor administrators' adherence to web browsing restrictions on servers.

Groupware Services has applied the SCW to all upgraded UMROOT infrastructure servers, and has begun applying it to non-upgraded servers as well. Policy to limit web browsing on servers is in place.

- Justification of Privileged Accounts - The Privileged Account Policy listed and defined the powers of privileged AD groups without specifying which teams or job roles should belong to each group. Management planned to extract the memberships of the various privileged groups and document the precise makeup and the reasons for inclusion so that privileged access is clearly justified.

Monitoring of privileged groups has been increased. The Windows group receives an automated report of privileged group membership via email every Monday and Friday morning, and reviews it for suspicious changes. The Windows group also receives automatic email alerts whenever an account is added to these privileged groups, providing continuous monitoring. Management still plans to document the precise makeup and reasons for inclusion in privileged groups and finalize the Privileged Accounts Policy.

- Caching of Domain Credentials - Domain credentials could be cached on servers and workstations in the UMROOT domain. If a workstation containing cached credentials of privileged accounts were compromised, the domain would be at risk. Management had amended the Privileged Accounts Policy to forbid logging on directly to workstations or member servers with a privileged account. They had discussed the policy change internally, and planned to issue a final announcement via email to all affected system administrators.

Management has sent email to the LAN/NOS team notifying them of the policy to use Domain Administration accounts only to log in to Domain Controllers, never workstations or member servers. They have also developed a new procedure for situations requiring non-conforming use of Domain Administration accounts, in which temporary administration accounts are created and then deleted immediately after use. Membership of the Domain Administration group is monitored continuously, sending out e-mail alerts whenever an account is added to the group (also discussed in the previous item). The staff member then replies to the alert with an explanation of the activity being performed that requires the temporary account.

- Absence of Operating Level Agreement - There was no operating level agreement (OLA) documenting the level of service the UMROOT Domain provided to members of the Campus Forest. At that time, the Windows Leadership Group had just agreed to collapse non-UMROOT domains into UMROOT organizational units (OUs), which would significantly alter the relationships and responsibilities documented in an OLA. Groupware Services planned to develop an updated agreement reflecting the planned restructuring.

A table describing the abilities and responsibilities of AD units has been created and shared with members of the Windows Core Working Group. The document delineates the roles of the forest maintainers (ITS staff), domain owners, and OU owners that will form the basis of the OLA. Domain owners built a list of capabilities they require to function in the newly collapsed forest. The Windows team will develop an OLA for the collapsed campus forest, incorporating relevant portions of the "AD Units Abilities and Responsibilities" table and the forest requirements list. The team will also revise security policies for the collapsed forest.

- Informal Change Management - Changes affecting the entire UMROOT domain were largely informal, not based in policy, and required better integration and documentation. Groupware Services planned to examine available options for unifying its change documentation and approval processes, including the Remedy system used by ITCom and the FootPrints service offered elsewhere in ITCS. The selected process or system would simplify tracing the history of specific changes, and provide assurance that changes are suitably vetted, approved, and communicated.

Before ITCS combined with other units to form ITS, Groupware Services met with ITCom to discuss their change management practices and the possibility of jointly developing a process. The formation of ITS has presented more options. LAN/NOS Groupware Services is documenting the current change process, and will investigate and adopt the best change management capabilities available within ITS.

- Disaster Recovery Plan - Disaster recovery procedures were technically thorough but did not address certain broader operational issues such as actual disaster scenarios, coordination of recovery efforts, communication methods, and how the plan will be tested and kept current. Groupware Services planned to incorporate the recommended elements into the UMROOT disaster recovery plan as it was rewritten for Windows Server 2008. They also planned to establish a periodic schedule (every one to two years) for reassessment and retesting of the recovery process, including documentation of lessons learned and any revisions to the plan.

LAN/NOS Groupware Services has developed and tested backup and restore procedures for the Windows 2008 environment. They are still developing a complete disaster recovery plan that will incorporate additional elements, including the personnel involved and communication plans. ITS leadership has separately acknowledged and supports the establishment of disaster recovery plans for all critical systems.

DPS Management has taken appropriate action to strengthen controls and address issues discussed during the audit. Details regarding the implemented corrective actions are noted below. **This audit is closed.**

- Internal Recharge Rates - DPS Management has performed a detail analysis of the recharge rates they use to bill U-M units for law enforcement and security services. The Office of Financial Analysis reviewed and approved these internal billing rates as of June 16, 2009.
- Procurement - DPS management made several changes that strengthened controls over the procurement process and ensure consistency with University, Facilities and Operations (F&O), and DPS guidelines. At present, support personnel from DPS Chief's Office, Field Operation Services, Communications, Technical Services, and Staff Operations maintain original documentation of all purchases made for their respective bureaus until the Statements of Activity (SOA) and P-Card statements are reconciled each month. Reconciled SOA and P-Card statements are further reviewed and approved by authorized DPS personnel. The reconciliation and review process is adequately documented. Once reconciled and reviewed, the statements and the original supporting documents are forwarded to the DPS Senior Financial Clerk for processing and central filing. DPS management is maintaining adequate documentation of the approval of hosting charges in accordance with F&O and DPS policy.
- Grant Management - DPS management has strengthened controls over the grant management process by taking the following actions:
 - Reconciling and reviewing their project grant specific SOAs on a regular basis to ensure accuracy, appropriateness, and completeness of financial reporting. DPS senior financial clerk is using the sponsor provided guidelines to ensure expenses are in line with project grant requirements.
 - Maintaining adequate documentation to support grant related expenses. These supporting documents clearly state the purpose of the expenses and refer to the grant used to pay for the expenses.
- Tracking Mandatory Training - Management has not yet implemented an automated process to efficiently ensure that each DPS staff member is completing required training and career development programs. However, DPS has exhibited substantial progress on their action plan. Management has identified suitable training management software and attended a software demonstration event in August 2009. DPS management is awaiting a price quote from the vendor.
- Inventory Audit Documentation - Per DPS internal policy, management performs an annual audit of all department-owned equipment. Results of each inventory audit are reviewed and analyzed by management to determine if any items have been lost, stolen, destroyed, or become obsolete or inoperable. DPS management has improved their inventory audit documentation process by recording the date of the inventory audit and the name of the person who performed the audit.

University Human Resources Benefits Administration Office Follow-up Review

#2009-101

Original report issued April 30, 2009

Follow-up report issued September 30, 2009

A follow-up review was conducted to determine the status of management action plans. The majority of plans have been completed and significant action has been taken on plans in progress. In- process plans will be reviewed for implementation status during the third quarter of FY 2010. Individual action plans status is discussed below by key process.

SET PREMIUMS AND MANAGE SELF-INSURED PLANS

- Plan Administrator Transparency - Quarterly meetings have been established between BAO management and the University of Michigan Health System Contracting Director in an effort to

partner for greater transparency in administrative contracts and more timely estimates of hospital settlements to the U-M medical plans. The Contracting Director will provide data and estimates for University of Michigan Health System hospital settlements. An amendment to the Blue Cross Network (BCN) administrative service contract, including changes requested by the Office of the General Counsel and the University of Michigan Health System Contracting Director is pending signature of the Assistant General Counsel. **This issue is closed.**

- Internal Controls Documentation: Policy and Procedures - A project plan to maintain the internal controls directory is completed and well documented. Work efforts have been initiated with an expected completion date of March 31, 2010. All managers are scheduled to complete Fiscal Year 2010 annual reviews for their specific areas. Policies and procedures will be formally reviewed by the designated manager, BAO Director, and BAO Associate Director for Finance annually, on a rotating schedule by area. Major changes in policy and procedure will be reviewed and updated on an ad hoc basis through the year. A key process indicator report review will be performed for each plan type and functional area. **This issue is closed.**

ENSURE ACCURATE AND RELIABLE BENEFITS DATA

- Recurring System Issues - The BAO Director and the Assistant Director, HR Management Systems Products and Services have charged a committee to review BAO Systems post-transaction detective processes for opportunities to improve service and efficiency through corrective processing in the M-Pathways system before they impact internal or external customers. The BAO Assistant Director for Systems documented review procedures and criteria for moving processes to the production system. The BAO Assistant Director and the ITS Product Manager have met and documented their decision logic for the disposition of each current BAO corrective process. This information has been provided to the BAO Director and the Assistant Director of HR Management Systems Products and Services. **This issue is closed.**
- Logical Access to Benefits Data - The BAO Assistant Director for Systems has developed detailed reports of BAO employee access to M-Pathways Human Resources and Financial data sets for review by department managers. The Assistant Director has enhanced these reports by including descriptions of the M-Pathways panel pages that describe the data being accessed. Reports for all BAO personnel have been issued and meetings are being conducted with managers to review the appropriateness of their employees' access. Procedures for this annual process have been documented. **This issue is closed.**

FACILITATE ACCURATE PREMIUM PAYROLL DEDUCTIONS

- LTD Participation in Discrepancy Reporting - The \$75,000 discrepancy identified during the audit has been explained as the difference between benefits payment amounts collected into a payroll account and the amounts transferred from the payroll account to an investment account on a monthly basis. At year-end, the residual amount remaining in the payroll account is transferred to an investment account.

The Discrepancy Reporting process identifies differences in payroll deductions and benefit enrollee data. A working group consisting of Payroll, Benefits, and ITS members is analyzing the cost-benefit of including the Long Term Disability (LTD) plan in the Discrepancy Reporting process. The BAO Assistant Director for Systems performed manual procedures to estimate costs and project potential LTD discrepancies. Payroll and ITS members are developing estimates for their time to develop procedures and programming in support of LTD discrepancy reporting. The group will meet again in late September to make a recommendation to management. **Outcomes for this action plan will be reviewed and reported as part of a second follow-up.**

PAY BENEFITS VENDORS

- Invoice Error Reporting - The data required for determining that all invoiced claims are made for a University qualified beneficiary at the time of service has been obtained from BCN, SXC (pharmacy vendor), and Blue Cross Blue Shield-Michigan (BCBSMI). Delta Dental data is being evaluated and the Strategic Health and Productivity Solutions (SHPS) pre-tax spending account claims data should be received by the end of September. Written procedures for performing audits, including processing methodology are complete. Testing for first quarter data is completed for BCN and discrepancies are being investigated. Based on the first complete set of results for all plans, BAO management will make a cost-benefit decision regarding continuation of the process. **Outcomes for this action plan will be reviewed and reported as part of a second follow-up.**
- Flexible Spending Account Payment Reconciliation - Interim reconciliation procedures are implemented and will promptly identify discrepancies between total vendor invoiced claims and total BAO payments on a monthly basis. Long-term procedures to verify eligibility will be implemented when electronic data is furnished by the plan administrator or when a new plan administrator is selected. The requirement for electronic data is incorporated into a request for proposal as part of the procurement process to renew or replace the expiring contract with the current vendor by calendar year 2011. **This issue is closed.**
- Consistent Record of Payment to Vendor - Wire transfers of retirement funds to banks are now initiated through non-PO vouchers rather than journal entries so that payments are associated to the vendor names in M-Pathways system records. **This issue is closed.**

COMPLY WITH BENEFITS LAWS AND REGULATIONS

- Compliance Monitoring - The BAO Benefits Compliance Administrator will develop and update the laws and regulations grid by October 2009. The grid will be expanded by end of March 2010 to include procedures that ensure compliance to each of the laws and regulations, including audits, testing, and monitoring. This process is included as part of the BAO project plan for developing and updating all key BAO policy and procedures. **Implementation of this action plan will be reviewed during the second follow-up.**

MANAGE BAO OFFICE ADMINISTRATION EXPENDITURES

- BAO SOA and GPR Reconciliations - BAO management and the University Controller agree that the current, BAO-developed electronic reconciling process effectively meets BAO needs. The intermediate accountant that developed and runs the reconciling reports does not have procurement access and a second individual is capable of running the BAO reports as a back-up. Segregation of duties and back-up are now formalized in written procedures. Beginning with September statements, BAO management will require evidence of reconciliation of the report totals to M-Pathways SOA totals. Management will also perform a sample review of supporting documentation and document these reviews in the monthly management meeting notes. **This issue is closed.**
- Spreadsheet Application Documentation - BAO spreadsheets that support business transactions and analysis have been restricted for read/write access to the Accountant Intermediate, Financial Analyst Senior, and the BAO Associate Director for Finance. The spreadsheet application processes now include documentation of data sources and locations and a flow diagram of procedures. **This issue is closed.**

**Open Audits Follow-up Table
September 30, 2009**

Audit Title	Report Date	Issues	Expected Completion
College of Engineering Research Computing 2008-302	10/29/08	Vulnerable systems; unnecessary services; unknown ports and services; unknown systems; unsupported devices; users with system administrator privileges; updating firewalls; procedural documentation	First Follow-up September 2009
			November 2009
Michigan Administrative Information Services Grade System: Web-based Grade Changes 2008-114	12/23/08	Role assignments; customization; two-factor authentication	First Follow-up September 2009
			November 2009
Housing Information Technology Office Residential Housing Network 2009-309	5/28/09	Registration scans; patching through portal; vulnerable systems; traffic analysis; incident response procedure; signed service agreements	November 2009
University of Michigan Hospitals and Health Centers Cashier's Office 2008-206	10/17/08	Segregation of duties; bank statement reconciliation and check writing practices; follow-up of outstanding vouchers; duplicate facility refunds	First Follow-up June 2009
			December 2009
UMHHC Payroll and Timekeeping 2008-110	1/30/09	Human Resource Management System access; systematic data integrity; payroll expenditure analysis; roles and responsibilities	October 2009
Medical School Administrative Internal Control Review 2008-208	1/30/09	IT strategic planning; reconciliations; gift fund usage; IT security; fire drill regulations	December 2009
Resident Duty Hours 2008-102	1/30/09	Duty hours compliance	October 2009
Children's and Women's Hospital Construction Audit 2009-601	4/02/09	Establishing guaranteed maximum price; sales and use tax; retaining payment documentation	December 2009
University of Michigan Health System Cardiovascular Center Supply Chain Audit 2009-105	5/15/09	Blanket purchase orders; inventory tracking; drug management; patient billing; system access; policies and procedures	January 2010
University of Michigan Hospitals and Health Centers East Ann Arbor Ambulatory Surgery and Medical Procedures Center 2009-208	07/28/09	Time reports; P-Card holder profiles; unsecured credit card terminal; building security	March 2010

UMHS Clinical Research Billing 2009-402	9/30/09	Research Planning; integrated solutions; interim solutions; policies and procedures	June 2010
Plant Operations Construction Services 2008-602	11/4/08	Project management reporting	First Follow-up June 2009
			February 2010
School of Music, Theatre & Dance Fiscal Responsibilities 2008-815	11/26/08	Financial oversight and monitoring; several procurement and payroll observations; documented procedures; written delegation of authority; imprest cash management	First Follow-up August 12, 2009
			December 2009
William L. Clements Library 2008-212	1/26/09	Grant compliance; endowment agreements; collection management; insurance coverage; physical safety and security; reconciliations; recharge rates	February 2010
University Press Inventory and Receivables 2008-203	1/30/09	Accounts receivable; inventory	February 2010
School of Kinesiology Fiscal Responsibilities 2009-203	4/14/09	Effort reporting; SOA and gross pay register reconciliation and review; credit card terminal placement; time reporting review; imprest cash fund; deposits; record retention; background checks; hiring documentation	December 2009
Benefits Administration Office 2009-101	4/30/09	Logical access to benefits data; addition to discrepancy reporting; invoice error reporting; flexible spending account payment reconciliation; compliance monitoring	First Follow-up September 30, 2009
			March 2010
University of Michigan – Flint Office of Development and Alumni Relations and University Outreach 2009-811	5/15/09	Relationship with University Development; performance standards; prospect management; coordination with Schools; cash handling; pledges; budget process; business continuity/disaster recovery plan	February 2010
University Unions Focused Review 2009-809	6/01/09	Cash management; payroll observations; statement of activity reconciliation; computer access	October 2009
Chemical Biology Doctoral Program Interdepartmental Degree Program 2009-812	6/30/09	Program reporting and oversight; compliance with procurement and hosting guidelines; effort certification; record retention; service level agreement; conflict of interest and conflict of commitment	February 2010
Deposit Process Audit 2009-103	07/20/09	Tracking of bank errors/adjustments; foreign checks; automated deposit stations security; treasurer's office procedures	December 2010
Dearborn Early Childhood Education Center 2009-110	09/30/09	Aged A/R; timeliness of deposits; physical security of cash; reconciliations; receipts; hosting events documentation; voucher review; privacy of employee records; double-time; IT security	March 2010