

UNIVERSITY OF MICHIGAN

REGENTS COMMUNICATION

Received by the Regents
October 14, 2010

Item for Information

Subject: Report of University Internal Audits
July and August 2010

Background:

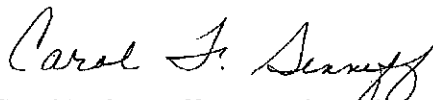
This is the report of the Office of University Audits activities for the period **July through August 2010**. The summaries of audits contained in this report were previously reported to members of the Regents' Finance, Audit and Investment Committee and included in discussions at Committee meetings.

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 **August 31, 2010**.

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

Respectfully submitted,



Carol F. Senneff, Executive Director
University Audits

University Audits
July - August 2010
Summary of Reports Issued

ORIGINAL REPORTS

Campus

PeoplePay

#2010-107

Report issued July 16, 2010

PeoplePay is a web-based decision tree that assists University administrators in choosing the correct payment mechanism for non-salary payments to employees and non-employees. The web tool does not process transactional data; it is a reference tool that refers administrators to the appropriate form and payment mechanism within Payroll or Procurement via hyperlinks. The long-term concept for PeoplePay was to transition to an integrated system that enables users to seamlessly process payment requests, regardless of method or type, via built-in workflows. Management is currently considering the feasibility of further integration with existing transactional systems.

University Audits' review was limited to assessing the tool's effectiveness in simplifying the payment process and ensuring compliance with related University policy and federal regulations.

Based on interviews and initial analysis the following objectives were developed:

- Verify PeoplePay oversight and change management are sufficient to serve the tool's intended purpose.
- Confirm the PeoplePay website contains sufficient explanation of intended use and system limitations to ensure proper use.
- Confirm sufficient process, procedures, and documentation exists to ensure adequate maintenance of the website.
- Verify instructions for payment type selection and processing are compliant with University policy and federal regulations, if applicable.
- Determine if monitoring and evaluation of system use and user experience is sufficient to maximize system efficiency and effectiveness.

Risk and Control Discussion:

1. Payroll Office Review - During the first three quarters of fiscal year 2010, over 7,000 payments totaling more than \$16 million of non-salary payments flowed through the Payroll Office. Three Payroll employees are responsible for identifying potential misuse of forms resulting in non-salary transaction errors. Current procedures include a review of submitted payment forms for:
 - Reasonableness
 - Proper withholding calculation for payees located outside of Michigan
 - Proper tax treatment of non-resident aliens

These review procedures are not documented and no formal exception reporting exists.

University Audits selected a sample of fiscal year 2010 payroll transactions and noted approximately 10% of the reviewed transactions were processed with the wrong earning code or payment method. In all cases, the Payroll Office eventually corrected the error, but only after notification from the unit that originally requested the payment. The complexity and

subjectivity surrounding the tax treatment of non-salary payments makes it difficult to develop effective exception reporting.

Management Plan - All of the central administrative offices involved in the PeoplePay functionality are committed to:

- Staffing the PeoplePay Lead Team
- Maintaining the PeoplePay web tool, as needed
- Developing training materials to facilitate the use of proper payment methods

The Payroll Office has expanded its review process to include all non-salary payments and will be documenting the procedures. The Payroll Office and Human Resources Records and Information Service (HRRIS) will investigate options for revising the current non-salary payment processes. Options for exception reporting will be researched.

2. PeoplePay Capabilities - The University community does not always understand the intended use and limitations of the PeoplePay tool. Many users believe that PeoplePay is a payment system rather than a reference tool. They mistakenly attribute sophisticated functionality and controls to the tool that do not exist, and inappropriately place reliance on the tool to enforce proper processing and authorization of payments.

Management Plan - The PeoplePay welcome page will be revised to attempt to clarify the web tool's intended use and limitations. References to PeoplePay on the Procurement and Payroll Services websites will also be revised. Training and communications with users related to PeoplePay will highlight and emphasize the tool's limited capabilities and the necessity to use the tool for each and every payment.

3. Change Management - Since its inception, PeoplePay continues to change to meet current federal and state tax law and users' needs. Edits to website content, payment forms, and hyperlinks are made frequently but no change management process exists to ensure approval, accuracy, and efficiency.

Management Plan - The PeoplePay Lead Team will:

- Document the change management process that supports the web tool.
- Enhance the tracking log to include the recommended additional information.
- Consult with Michigan Marketing and Design¹ (MMD) to develop standards for performance including acceptable turnaround times and the testing process.

4. User Feedback - Interviews indicated that PeoplePay users were generally pleased with the tool, which simplified the process for making non-salary payments to employees and non-employees. Administrators stated that there were fewer corrections and quicker payment turnarounds. They also said that department administrators have a better understanding of University policy by using the tool. The following opportunities for enhancements were identified:

- Add hyperlink to instructions on "grossing up" payments to account for tax withholding and ensure the payee receives a check for the intended amount.
- Include warnings about improper use of payment methods or types.
- Provide alerts related to University policy or system changes.

¹ Michigan Marketing and Design, currently provides web-site maintenance and support at the direction of the PeoplePay Lead Team.

- Supply contact information for questions. Some users with complicated and unusual payment scenarios prefer to talk with a subject expert over the phone or email rather than using the PeoplePay Lead Team's email group.
- Expand PeoplePay Procurement Tracker functionality to include payments processed through HRRIS and Payroll.

Management Plan - The PeoplePay Lead Team will work with MMD to investigate adding an alert mechanism when web tool changes are moved to production and a drop-down list that provides the recent history of changes. A hyperlink to instructions on "grossing up" payments currently located on the Payroll website will be added to the PeoplePay web tool in the text for paying awards and in the instructions for the "Payment to Non-employee for Taxable Services" form. It should be noted that the HR/Payroll Service Center and Procurement Customer Service phone numbers are already included in the PeoplePay "Contact Us" information. If Phase II for PeoplePay is implemented, flagging of common errors along with warnings about the use of improper payment methods will be considered during the design.

A formal follow-up to the outstanding issues will be conducted in the fourth quarter of 2011.

UM-Flint School of Education and Human Services Fiscal Responsibilities
Report issued July 19, 2010

#2010-812

The School of Education and Human Services (SEHS or the School) is one of the four schools of the University of Michigan at Flint (UM-Flint). The mission of SEHS is to prepare students for careers in education and human services by offering a variety of undergraduate and graduate degrees and several certification programs in these fields. Currently, the School is comprised of four departments: Department of Education, Department of Early Childhood, Department of Social Work, and the Early Child Development Center (ECDC).

The UM-Flint Chancellor requested an audit of SEHS because of a deficit the School had incurred over the past five years. This review was originally planned to be conducted in fiscal year 2009. At the request of the UM-Flint Provost, the audit was postponed until a new SEHS Dean was selected. The UM-Flint Vice Chancellor for Academic Affairs served as Interim Dean for a few months. The new Dean started in September 2009.

The objective of this audit was to determine if policies, procedures, and the internal control structure at SEHS are adequate to support the mission of the School and comply with University guidelines. The review focused on key fiscal responsibilities and administrative areas including:

- Financial reporting and budget
- Faculty course release time
- Student field placement
- Payroll
- International travel
- Procurement
- Conflicts of interest and conflict of commitments
- Gifts and grants

The review focused primarily on central processes in the Dean's Office. However, some processes and procedures specific to each academic department were reviewed, for example the processes related to student field experience and international programs. Due to the nature of their business, ECDC has unique risk areas such as transportation of children on field trips, compliance with state regulations for

childcare services, web cameras, billing and timekeeping systems specific to the childcare industry, and cash management. Findings and recommendations related to the processes specific to ECDC are being reviewed and reported as a separate audit.

Risk and Control Discussion:

1. Financial Reporting and Budget Monitoring - SEHS has incurred a deficit of approximately \$1 million dollars over the past five years. The primary reason for the deficit is a significant drop in enrollment at the School over this time. At the same time, SEHS expenditures have consistently exceeded their allocated budget. The growth of the deficit may be attributed to a lack of adequate procedures to monitor the budget and expenditures on a regular basis. Specifically, University Audits observed that:
 - Year-end projections are not consistently prepared during the year. Financial decisions are not always supported by adequate information; budget adjustments are not always made in a timely manner.
 - Budget-to-actual comparisons are not prepared and monitored. Budget variances are not explained and documented.
 - At the time of the review, the Statements of Activities (SOA) had not been properly reconciled in over a year. Errors and inappropriate charges may not be identified without comparing transactions to source documents.
 - The School's departments are not consistently provided with adequate, timely budget and financial reports. Therefore, financial decisions at this level may not be based on accurate information.
 - SEHS has already begun working with the UM-Flint Financial Services and Budget Office to more effectively utilize their account structure. This would allow for budget allocations to the department and program level and in turn improve financial monitoring and reporting. These efforts are complicated by the fact that small departments have to be supported by revenue generated from more mature and well-established departments. The current organization of the departments within the School may not fully support the efficient allocation of funding and the goals of financial solvency.
 - The School does not have adequate and sufficient resources to monitor the budget, prepare projections, and make recommendations to management. Currently, the School has only one Senior Administrative Assistant at forty-percent effort that is responsible for budget administration and financial analysis. Her remaining sixty percent appointment is as the Administrative Assistant at ECDC.

Management Plan - It is the intent of the Dean of the School of Education and Human Services (SEHS) to prepare a realistic budget for the SEHS that will allow for current operations to function optimally within reasonable budgetary limitations while allowing for purposeful planning for robust growth of the unit. Insuring that expenditures do not exceed allocated budget resources is a minimum expectation. Downturns in employment markets affecting education and social work may be forecasted in both the short and long-term but neither provide the accuracy nor the opportunity for the academic unit to respond in a reasonably quick time frame. Short-term and long-term budgetary planning for the SEHS must include program development that places the unit in a more risk-tolerant stance in order to weather inevitable market forces.

With that in mind, the Dean and Administrative Assistant Senior will follow the following action plan:

- Administrative Assistant Senior will work directly with Financial Services and Budget Office to examine historical data and future budget projections of revenues and expenses based on current academic program offerings.
- Monthly monitoring of budget expenditures, reconciliation of Statements of Activity (SOA), documentation of budget variances, and explanations for variances will be monitored by the Administrative Assistant Senior and reported to the Dean and chairs on a monthly basis in a monthly State of the Budget meeting.
- After consultation with the SEHS Stewardship Executive Committee, the Dean will determine whether the Early Childhood Education (ECE) Department should be subsumed under the Education Department. Currently, the ECE Department consists of one chair and one faculty member. In the interest of creating an equitable budget model across departments within the SEHS and in standardizing budgetary allocations, a department of two does not suitably serve the budgetary interests of the School.
- On-going, careful, and consistent monitoring of budgetary processes along with financial planning for growth and sustainability require full-time, dedicated support. Currently, the Administrative Assistant Senior is devoting forty percent effort to all SEHS budget monitoring. Her remaining sixty percent effort is devoted to work at the Early Childhood Development Center. Less than half-time work effort is not sufficient given the need for monitoring and planning for future financial growth. In addition, this individual's role serving the Early Childhood Development Center poses a conflict of interest and commitment between the SEHS and Early Childhood Development Center. In consultation with the Provost, the SEHS Dean will explore the feasibility of establishing a full-time position for an individual with budgeting, financial planning, and academic program development skills as a permanent, proactive response to the SEHS's long term fiscal growth.

2. Segregation of Duties - University Audits observed several instances where segregation of duties is not appropriate.

- Timekeeping - SEHS employees report time data by using the self-service feature in Wolverine Access. SEHS has designated the Executive Secretary to the Dean as the only approver in the system. Therefore, in some cases, she approves time for employees for whom she does not have direct knowledge of hours worked.
- Procurement - The designated reconciler of the SOA has purchasing responsibilities and access to the system, and therefore can control a transaction from start to finish.
- Children's Reading Center - The Reading Center provides opportunities for K-12 students in Genesee County to attend individualized reading classes with University graduate students. Parents of the children pay a fee for participating in this program. University Audits observed that an Administrative Assistant for the Department of Education bills parents, receives payments, and deposits the funds. A reconciliation of revenue to the billings is not performed.

Management Plan - As of June 30, 2010, the Education Department Chair took a position at another university and the SEHS Dean appointed an interim chair for the remainder of his term, expiring August 2012. For now, staff reporting lines will remain as they currently exist whereby the Executive Secretary to the Dean will serve as designated individual to approve time in the system. The current size of the SEHS unit makes segregation of duties challenging and, as a result, reporting lines need refinement. With that in mind, the SEHS Dean, in consultation with

department chairs and the SEHS Stewardship Executive Committee will engage in the following:

- Staff reporting lines will be reviewed for the purpose of streamlining and tailoring the structure of the Education Department's human resources. Until such time that any realignment of reporting may occur, the Executive Secretary to the Dean will continue to approve time but with written documentation of approval from the chairs of the Education and Social Work departments.
 - Since, in some cases, the same individual currently handles procurement and SOA reconciliation, the SEHS Dean will pre-approve any purchase over \$500. In addition, various solutions for segregating duties will be explored including, but not limited to, training current staff in specialized duties they would perform school-wide (i.e., one individual responsible for procurement, another for timekeeping, another for reconciliation).
 - Billing and collecting of payments for families enrolling children in the Reading Center will continue to be processed by the Education Department Administrative Assistant Intermediate but will be reconciled by the Administrative Assistant Senior.
3. Faculty Release Time - Faculty may be allowed release time from teaching one or more courses every semester to serve in positions such as department chairs, participate in advisory committees, coordinate accreditation efforts. The Dean of SEHS is the authority who reviews and approves release time for the School. University Audits observed instances where release time was not formally approved or properly documented.

SEHS can further improve controls related to release time. Specifically:

- Establish a formal process to approve faculty release time by an appropriate authority.
- Maintain adequate documentation of course releases in the faculty files in the Dean's Office.
- Formally document the release time policy for specific permanent positions (e.g., department chairs, graduate program director) and establish a general framework for course releases allowed for other sporadic positions (advisory committees, accreditation coordinators).
- Establish a threshold for the number of course releases per semester or year. Perform regular monitoring to ensure the amount of course releases is appropriate and not excessive.

Management Plan - The phenomenon of faculty release time is one that, historically, compensates faculty for work performed above and beyond that which is customarily expected. Due in part to the small size of the SEHS, much is expected of a small number of faculty fulfilling multiple roles. The increase in release time, while apparently not having been formally approved or documented and which may have been over-utilized within the SEHS, is linked to many forces that come to bear on professional schools seeking to receive state authorization, as well as to achieve and maintain national accreditation. Providing adequate coverage across all departmental, school and university-level committees, creating and sustaining lucrative new graduate programs, responding to state mandates, and achieving and maintaining accreditation require robust, sustained commitment that, in a larger unit, would be dispersed across a greater number of individuals. Clearly, until the unit grows in its number of faculty, the work must continue. In the meantime, the Dean will work in consultation with the SEHS Stewardship Executive Committee to address the control recommendations, as follows:

- All faculty release time must be approved, in advance, by the SEHS Dean.

- Up-to-date documentation of course release time will be maintained in faculty files.
- A general framework for course release time will be created and articulated for the SEHS Governing Faculty.
- A threshold for the number of course releases per semester and per year will be established and articulated for the SEHS Governing Faculty.
- Articulation of expectations for tenured and tenure-track faculty of all ranks will address that which is within and beyond what is customarily expected of faculty work load.

4. Conflict of Interest and Conflict of Commitment - SEHS follows the UM-Flint Conflict of Interest and Conflict of Commitment (COI/COC) policy. Staff members completed COI/COC disclosure statements in 2007. However, these statements have not been regularly updated since then. University Audits observed that some conflicts or potential conflicts were not properly disclosed and management action plans were not documented.

Management Plan - All SEHS staff and faculty will be apprised of the current tutorial on Conflict of Interest/Conflict of Commitment offered through the UM-Flint Human Resources Department. At the first regularly scheduled meetings of the SEHS Governing Faculty and SEHS staff, a Human Resources representative will be asked to make a presentation and provide copies of the form for distribution and signature by all faculty and staff. The Executive Secretary to the Dean will annually collect and keep signed documents on file.

5. Policies and Procedures - SEHS has documented policies and procedures for some areas. For example, policies and procedures for student field placements are very well documented in both the Department of Education and Department of Social Work. However, other key operational procedures for SEHS are not formally documented. Because SEHS has limited resources, documented policies and procedures are critical to ensure business continuity.

Management Plan - Creation of formal policies and procedures guiding the SEHS is of utmost importance to the internal functioning of the unit. While policies and procedures exist, in some cases they have not been routinely or systematically followed. Since policies regarding budgetary matters are not separate from the work of faculty engaged in teaching, curriculum development, and new program development, the development and documentation of policies will involve a large number of individuals throughout the School. The SEHS Dean, in consultation with the SEHS Stewardship Executive Committee, chairs of the Education and Social Work Departments, Administrative Assistant Senior, and Executive Secretary to the Dean will do the following:

- Document existing policies and ascertain that they are being followed.
- Determine any current policy that may be outdated and eliminate it.
- Determine any need for policy development and then draft and implement it.
- Create an SEHS Business Policies and Procedures Handbook.

University Audits will conduct a follow-up review in the third quarter of fiscal year 2011 to assess the effectiveness and adequacy of internal control improvements implemented by management.

U-M Flint Early Childhood Development Center
Report issued July 19, 2010

#2010-118

The University of Michigan-Flint Early Childhood Development Center (ECDC or the Center) is an

education and childcare center for children from infants through preschoolers. It reports administratively to the UM-Flint School of Education and Human Services (SEHS). The primary mission of ECDC is to create a safe and suitable environment where young children can develop, learn, and grow. The Center serves both the University community and the Greater Flint area as parents of children enrolled at ECDC include University staff, faculty, and students, as well as members of the surrounding community. As part of the UM-Flint School of Education and Human Services, the ECDC provides undergraduate students with hands-on experience for teacher preparation and child study. Many education and early education students are employed at ECDC where they can interact with children and learn in a real-life environment. Many other students, particularly those enrolled in courses related to early childhood education and behavior, come to the Center to observe how young children interact with the surrounding environment.

ECDC first opened in October 2002. The Center is located in the William S. White building on the UM-Flint campus. The Department of Human Services (DHS), a State of Michigan department responsible for licensing all childcare centers in Michigan, licenses ECDC. This license is renewed every two years. ECDC's license was most recently renewed in June 2009. The Center is currently licensed for a capacity of 125 children.

In October 2008, the National Association for the Education of Young Children (NAEYC) accredited ECDC. The NAEYC is a not-for-profit association that, among other things, accredits early childhood programs according to its health, safety, and education standards. This accreditation is voluntary. NAEYC revised its standards in 2006 to provide a more reliable and accountable accreditation system and to encourage new levels of excellence in the field of early childhood education. ECDC was one of the first childcare centers in the United States to obtain accreditation under the new standards.

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

- Field trips
- Cash management
- Information technology
- Financial management
- Compliance
- Payroll
- Procurement

Risk and Control Discussion:

1. Financial Decision-making - As an auxiliary unit, ECDC receives limited general fund support from the School and is primarily supported by revenue generated from tuition, fees, state funding, and grants. Many important financial decisions for the Center are made without communication, consultation, or approval from a higher administrative authority at the SEHS. University Audits observed several instances where financial decisions are made in isolation. For example:
 - A higher administrative authority does not review and approve rates charged for tuition and fees. ECDC has not revised these rates in several years. The Center may be missing opportunities to increase their revenue while still being competitive in the market.
 - ECDC has a policy that states that late fees should be charged to parents who fail to pay their account balance on time. However, ECDC management does not actively charge

late fees. By not charging late fees, the Center fails to set an appropriate tone with their customers regarding timely collections.

- A higher administrative authority does not periodically review accounts receivable. ECDC has a policy that states that children can no longer attend the Center if the overdue balance reaches \$500. However, several accounts have passed this threshold during the current fiscal year. Overall, ECDC has a significant amount of uncollected receivables over the past eight years. Analysis of these accounts is not regularly performed and aging reports are not detailed enough to show trends over time.

Management Plan - In order to improve communication and oversight, the Dean and ECDC Director will begin monthly meetings where the Director will provide updates on day-to-day operations including budgetary matters. The first meetings will focus on review of current tuition rates, policies regarding late fees and collections, and charitable care. A set of financial goals will be determined based on review of the current tuition rate and determination of whether an increase would be financially prudent at this time.

Annually, a review of tuition rates will occur in order to make adjustments appropriate to the ECDC's policy in serving the community, market forces, and financial goals. In consultation with the ECDC Director and other key Executive Management-Flint areas, the Dean will approve tuition rates. With respect to changes in policy or waiving of a policy in special cases, the ECDC Director will consult with the Dean to obtain prior approval.

The ECDC Director will work with UM-Flint Financial Services and Budget Office to establish guidelines and parameters for uncollectable accounts, including when accounts are reported to collection agencies and when uncollected accounts are written off. The Dean will pre-authorize any write-offs. The Dean will periodically review receivables, write-offs, and their trends over time.

2. Kid's Care System - ECDC uses Kid's Care, an electronic system, to manage the Center's finances and timekeeping. This system is composed of two separate applications: an Access database where ECDC records clients' information and financial data and a DOS-based database where ECDC records client and employee time. The data stored in Kid's Care is of significant importance to the Center's financial operations. The parents' records in the financial database include family information, billing records, and payment history. Time records include the hours each child is in attendance at the Center. This data is used to bill parents, as well as to provide DHS with attendance reports. Employee time data is used to generate payroll for ECDC employees. University Audits observed several issues with the system. Specifically:
 - The financial database is located on the hard drive of a desktop computer and data files are not regularly backed up. ECDC may lose their financial history if the hard drive fails.
 - The timekeeping application does not have the ability to generate certain reports necessary for ECDC reporting to DHS, such as average daily attendance reports. An administrative assistant manually calculates the daily average attendance. This process is inefficient and time consuming.
 - The timekeeping application files cannot be saved electronically. Hardcopies of all the records are prepared on a monthly basis. The system automatically deletes records older than one month. The Center risks losing the data if the hardcopy reports are not prepared in a timely manner. The process of preparing and saving these reports is also inefficient.

- The database does not provide different access levels that would allow for proper segregation of duties in the system. Currently, three ECDC employees have the same level of access to the system with a common user name and password. These employees also have financial responsibilities related to customer billing and payments, cash handling, reconciliations of revenues and expenses, and financial monitoring. The system does not provide audit trails or logs of changes made to customer accounts. Because of these system limitations, management review and oversight for changes to customer accounts may not be appropriate.

Management Plan - Upgrading the ECDC's data management system is of utmost priority and, to that end, the following is currently underway:

- The Kid's Care financial management system is now backed up every Monday morning on the Administrative Assistant Senior's H drive. Further, the H drive is backed up daily by the UM-Flint ITS.
- The Administrative Assistant Senior is currently checking with the vendor of the Kid's Care System to determine cost for upgrades that will allow for advanced timekeeping and for creation of a range of reports necessary to monitor operations. In the unlikely event that the Kid's Care upgrade is cost prohibitive, exploration of an affordable software management system will be undertaken. Transition to the upgrade/new software system will take place prior to the start of the fall semester.

3. Web Cameras Access - ECDC has installed web cameras in all the children's rooms and playground areas. The purpose of the web cameras is to give parents and relatives the opportunity to see the children at any time. This is part of the Center's "open doors" philosophy as well as a marketing tool for ECDC. The live stream video from the cameras can be accessed by a common username and password. ECDC provides the username and password to the parents when the children first start at the center. The username and password have not been changed since the Center's cameras were set up in 2002. Therefore, individuals who no longer have children at the ECDC can inappropriately access the video. This may result in parental concerns over who can view their children and may create an unnecessary reputational risk for the Center.

Management Plan - Security of access to the web cameras is essential and, to that end, the following action will be taken:

- The password to the web cameras will be changed three times per year coinciding with the start of the fall, winter, and spring/summer semesters.
- Families with children enrolled in the ECDC will be notified of the changed password at the start of each semester.

4. Transportation Agreements - As part of their activities, ECDC organizes field trips for children outside of the Center's classroom building. DHS has specific rules regarding transportation of children. ECDC uses two service providers for transportation during field trips. The two providers are Mass Transportation Authority (MTA), a public service provider, and First Limo, a private company. DHS transportation rules apply when a childcare center uses an outside provider. Vendor noncompliance with the DHS transportation rules may result in potential risks to the safety of the children. In addition, failure of the service providers to comply with DHS rules and statuses may place the Center's license in jeopardy.

Management Plan - The ECDC will provide the DHS transportation guidelines to MTA and First Class Transportation management prior to the next time their services are utilized. In

addition, the ECDC will create a form for the agency to sign indicating an understanding of the rules and compliance with DHS transportation rules when providing services to the ECDC. The form indicating compliance will be updated annually.

5. Imprest Cash and Snack Station Fund - ECDC maintains a small station with snacks and beverages in the Center's reception area for the convenience of employees, parents, and visitors. ECDC charges minimal fees for these items. Cash collected is not deposited in the Center's University account, but is used to replenish the snack station inventory. Inventory is usually purchased with employee personal funds and the employees are reimbursed from the cash on hand. In reviewing controls for the snack station petty cash, University Audits observed that the fund is not officially documented with Accounts Payable as required by University policy. On occasion, the fund is used to make change for parents, to reimburse other miscellaneous employee expenses (e.g., travel expenses), and to purchase items in support of the Center's daily operations.

Management Plan - While the operation of the snack station has provided a level of convenience for parents and staff in obtaining refreshments, the necessary segregation of duties required for its daily operation, given the number of staff and available time, is not reasonable. The Dean will work with the ECDC Director to eliminate the snack station.

Procedures and controls reviewed as part of this audit ensure child safety and security within and outside of the Center. Management has established a culture of compliance with DHS rules and regulations. Minor citations are addressed promptly and adequately. The Center has developed a Staff Handbook of policies and procedures that is used for reference and training.

University Audits will conduct a follow-up review during the second quarter of fiscal year 2011.

Information Technology

Medical Center Information Technology Michigan PGIP Analytics Collaborative
Report issued July 16, 2010

#2010-302

University Audits has completed an audit of the Michigan PGIP² Analytics Collaborative (MPAC), a partnership between Medical Center Information Technology (MCIT), the primary IT service provider for the U-M Hospitals and Health Centers (UMHHC) and Blue Cross Blue Shield of Michigan (BCBSM). The purpose of the partnership is to analyze healthcare claims data and develop software tools to identify best practices that will improve outcomes and increase efficiency for physician organizations throughout Michigan.

MPAC was established by means of an agreement between U-M and BCBSM. Because U-M is receiving patient protected health information (PHI) from BCBSM, U-M is treated as a business associate³ of BCBSM in a HIPAA regulatory context. BCBSM treats the MCIT project staff as contractors. This arrangement is uncommon for U-M. It has merited lengthy review by the Health System Legal Office, Compliance Office, and Contracts and Procurement.

² PGIP (Physician Group Incentive Program) is an incentive program that connects physician organizations from across Michigan to encourage information sharing about various aspects of healthcare. Program participants collaborate on initiatives designed to improve the healthcare system in Michigan. *Source: BCBSM web site*

³ HIPAA defines a *business associate* as an individual or corporation, not a member of the covered entity's workforce, who is performing on behalf of the covered entity any function or activity involving the use or disclosure of protected health information (PHI).

As originally conceived, MPAC was designed to process data from a variety of providers. This plan was later amended so only BCBSM data was to be analyzed. This change resulted in a significant scaling back of the database used for analysis and a change in where it was housed. Due to these changes in the scope and makeup of MPAC, a restated agreement is currently being created. Negotiations for this restated agreement are ongoing.

An Executive Oversight Committee (EOC) with representation from U-M and BCBSM governs MPAC. The EOC reviews and approves project ideas. Either BCBSM or U-M proposes work in the form of a documented production project initiative (PPI⁴). The EOC approves it, and MCIT and BCBSM work together to execute it. The actual work product generated depends on the nature, complexity, and quantity of PPIs that are approved by the EOC.

This audit examined the project's administrative record keeping, systems security, and procedures necessary to comply with the contractual agreement, expressed legal and regulatory requirements, and University policies.

Specific audit objectives included verifying:

- Establishment and operation of governance bodies
- Retention of appropriate documentation of PHI access and use
- Documentation and assessment of the security of U-M systems involved in the project
- Clearly defined contractual terms and obligations

The primary risk with this project centers on the contract between U-M and BCBSM and whether its terms are reasonable and whether U-M is prepared to prove fulfillment of its obligations if BCBSM were to exercise its right to audit. Two of the most significant U-M obligations are protecting the confidentiality of BCBSM PHI and notifying BCBSM of security breaches of U-M systems where copies of BCBSM data are stored.

Risk and Control Issues:

1. Risk Assessment of Local Data Workspace - Under terms of the proposed MPAC restated agreement currently under negotiation, U-M is responsible for using appropriate administrative, physical, and technical safeguards to preserve the integrity and confidentiality of BCBSM PHI, using the same degree of care as for U-M's own confidential information.

Although most processing is done in BCBSM databases, copies of MPAC data are stored on a limited number of U-M managed systems. These include a small number of MPAC team workstations and an MPAC database schema⁵. The MPAC schema, which stores working copies of BCBSM data, shares both the Oracle database infrastructure and the administrative processes of the Health System Data Warehouse (HSDW).

Risk assessments for the MPAC database schema, HSDW, and supporting database infrastructure have not been completed. A database infrastructure risk assessment is partially complete but on hold while Medical Center Information Technology (MCIT) Compliance

⁴ The document or set of documents that captures the agreed upon purpose for UM's data use or disclosure and sets forth the associated work activities, deliverables, data elements, definition of tools and architecture, or other such information as necessary to document the collaborative effort between BCBSM and UM on a particular production project.

⁵ An Oracle schema is a collection of database objects such as tables, views, and indexes that contain or reference user data.

obtains additional personnel. The HSDW was not previously identified by management as a critical application; therefore, no risk assessment of it has been planned or completed. In the absence of risk assessment, security weaknesses in these systems and components may go undetected and could be exploited by intruders to compromise the confidentiality of PHI.

Management Plan - Risk assessment of MPAC schema and HSDW environment will be scheduled and prioritized appropriately by MCIT Compliance.

2. Project Governance - The draft of the restated agreement between U-M and BCBSM describes the governance model for MPAC, which centers on an Executive Oversight Committee (EOC). The makeup, operation, and responsibilities of the EOC are defined in detail. The EOC has been in operation for over a year, but some of its responsibilities have not yet been fulfilled. These include:
 - The EOC membership roster indicates that U-M currently has two clinical and three IT representatives on the committee. This configuration does not match the requirements of the agreement, which state the EOC shall include representatives from the following disciplines:
 - Clinical - two representatives from each Party
 - Information Technology - two representatives from each Party
 - Legal - one representative from each Party
 - An EOC charter has not been created. The EOC is required to “establish and agree upon a charter that establishes Michigan Physician Organization Common Data Resource (MPOCDR) governance, including but not limited to, quorum and procedures for bringing proposals to the committee” and review it at least annually.
 - An Advisory Committee has not been established. The EOC is required to “establish, provide administrative support to, and actively participate as members in an MPAC Policy and Oversight Advisory Committee (‘Advisory Committee’).”

The project appears to be functioning well in the absence of these elements and fulfillment of EOC duties is the joint responsibility of U-M and BCBSM as partners in MPAC. However, not having legal representation present at EOC discussions may hinder U-M's ability to make timely decisions when legal ramifications exist. Lack of a charter increases the risk of inconsistent EOC behavior. Lack of an Advisory Committee could hamper productivity of MPAC by limiting sources for project ideas.

Management Plan - MCIT will request that a representative from the Health System Legal Office be listed as an EOC member and attend EOC meetings as needed. MCIT will put the remaining items, including development of an EOC charter and establishment of the Advisory Committee, on the agenda of the next regularly scheduled EOC meeting.

3. Time Limit for Reporting Breaches - The Business Associate Agreement attached to the proposed restated agreement as Exhibit A states:

6.2 Should a (1) reportable Security Incident, (2) breach of PHI as described in §13400(1)(A) (42 U.S.C. §17921(1)(A) of the HITECH Act, or (3) unauthorized access, use or disclosure of PHI occur, UM shall provide to the BCBSM Privacy Official, within five (5) business days of the incident, a description of the event, the steps taken to mitigate the damage incurred, and any measures taken to ensure a similar event does not reoccur.

The UMHS Compliance Office, which would typically be responsible for this reporting, indicated it would be very difficult to complete all of the listed activities within five business

days. Information and Infrastructure Assurance offered a concurring opinion based on their experience coordinating security incident response on campus.

The Health System Legal Office indicated this deadline is not based on any legal or regulatory mandate, leaving it open to negotiation based on operational feasibility.

If U-M were unable to report a relevant security incident, including corrective action, to BCBSM within the contractually specified five business day period, under these terms U-M could be found in breach of contract.

Management Plan - MCIT will negotiate new incident reporting terms with BCBSM and incorporate them into the proposed restated agreement.

4. Control of Data Use/Access/Disclosure - The proposed restated agreement contains several requirements for the governance and review of data access, use, and disclosure. Some of these requirements have not been met and would be issues if the proposed agreement were ratified.
 - U-M has not prepared written policies and procedures governing disclosures to program participants and physicians that establish:
 - Role-based access to the MPOCDR and access termination conformant to Exhibit A (Business Associate Agreement)
 - Rules for inclusion or exclusion of identifiers of physicians, physician practice units, and physician organizations
 - U-M has not produced the required internal MPOCDR access, use, and disclosure governance policy stating that U-M shall only access and use other PGIP Participant data when engaged or invited to do so in a consulting context or when agreed to by BCBSM through an approved PPI or an approved motion presented to the MPAC Executive Oversight Committee. In the absence of policy governing use of other participants' data, project staff may use that data without appropriate permission.
 - U-M is recording activity involving BCBSM PHI in the form of database connection logging. However, that activity is not being reviewed on at least a quarterly basis to identify any actual or suspected unauthorized access to or disclosure of PHI as required by the Business Associate Agreement. Unauthorized access to MPAC data stored by MCIT may not be promptly detected without systematic review of database connection logs.

Management Plan - To comply with Section 10.1, MCIT will develop disclosure policy and procedures in conjunction with the first PPI that requires disclosure of MPOCDR data to program participants and physicians. These policy and procedures will be in place before any disclosures occur. MCIT will similarly comply with Section 10.2 by developing policy and procedures governing U-M's access and use of other PGIP Participant data in conjunction with the first PPI involving such data. MCIT will begin reviewing connections to the MPAC schema on a quarterly basis to identify inappropriate access.

A formal follow-up will take place in the third quarter of fiscal year 2011.

College of Literature, Science and the Arts Research Computing
Report issued July 27, 2010

#2010-809

The College of Literature, Science, and the Arts (LSA) is the largest college at the University of Michigan. LSA is home to more than seventy departments and programs. Most of these programs have

faculty engaged in some form of research. Despite the large research community, centrally provided resources, such as data storage, are not prevalent.

LSA's technology infrastructure is supported by the LSA Information Technology (LSA IT) department. LSA IT offers security services for faculty, staff, and students; and is the primary IT administrator for twenty-four of the departments within LSA. Additionally, many of the departments within LSA have their own IT staff to supplement the services provided by LSA IT. The level of support and services provided differs greatly between departments. This is due to the vastly differing needs of each department's users. Tasks usually handled by departmental IT teams include desktop support, system maintenance, and network storage. LSA IT is typically utilized for all other IT services such as networking, security, and system images.

Of particular note is the impact that LSA IT's Research Systems Group (RSG) and IT Security and Asset Management (LSA-Sec-ITAM) teams have on the research community. RSG provides a high performance computing cluster, multiple Linux load sets⁶ and application packages, and a variety of network services to both researchers and departmental IT staff. LSA-Sec-ITAM offers security services that include incident response, tracking, and reporting, as well as regular vulnerability scans. LSA-Sec-ITAM also monitors network traffic across all LSA networks.

Despite this robust IT infrastructure, many researchers manage their own systems. This audit focuses on the systems managed by researchers or their designees, not IT professionals. These systems are referred to as "unmanaged" machines.

This audit included examination of computers used for research at eight departments within LSA:

- Chemistry
- Geological Sciences
- Physics
- Molecular, Cellular, and Developmental Biology
- Psychology
- History of Art
- Economics
- Sociology

The objective of the audit was to evaluate risk relating to the computer security, data management, system configuration, and system administration practices and controls by performing the following:

- Surveying departmental IT administrators
- Surveying researchers
- Performing vulnerability scans
- Assessing college and department level policies
- Assessing college and department level practices and procedures

Failure to effectively manage risk related to research computing at LSA could result in:

- Loss of critical research data
- Exposure of sensitive data
- Compromise of University servers
- Compromise of University workstations
- Compromise of University networks
- Negative publicity for the University

⁶ A load set is a preconfigured operating system that includes a predetermined set of installed applications

Risk and Control Issues:

1. Security Policy - A security policy outlines acceptable users for both individual systems and the network as a whole. A good security policy will encourage users to better protect themselves and their colleagues on the network. Many departments within LSA have no security policy and rely solely on LSA IT's security policy for defining acceptable behavior. Departmental policies reviewed during this audit were of varying quality. While LSA IT's policy is well written, it does not address unique situations that would be covered by a local, departmental policy.

Department level IT teams should create their own security policy to supplement the policy provided by LSA IT. The departmental security policies should directly address any unique situations not expressly addressed in the LSA IT policy such as data classification, access control, virus prevention, intrusion detection, internet security, systems security, acceptable use, and any relevant exceptions.

Management Plan - LSA IT Security and the LSA Joint IT Research Committee will create a template for departmental IT staff to use to develop a comprehensive security plan that would cover all unique security concerns. This template will be distributed throughout LSA so department's can utilize it to create policies that meet their individual needs.

2. Data Classification - The departments within LSA represent a great variety of academic disciplines. Therefore, there is a variety of research data to be managed. Different types of data require different levels of management, security, and control. Data that is sensitive requires more security protection than data that is not as sensitive. Researchers currently have no guidance to help them determine which data is sensitive. Without this guidance, there is no clear indication for when they should be seeking help to secure their data.

Management Plan - LSA Joint IT Research Committee will review the current data classification guidelines provided by ITS to determine if they are current and accurate, and will utilize them if they are applicable. If the documentation provided by ITS is not sufficient for the needs at LSA, new documentation will be created. This documentation will define sensitive data and provide guidelines on how to protect it. The LSA Joint IT Research Committee will determine an effective method of delivering the information to the researchers and IT staff within the departments.

3. Data Storage - Many of the researchers contacted during this audit work with very large data sets, which creates unique storage problems. To solve these problems, researchers often purchase their own additional storage instead of utilizing other solutions provided by the department, college, or University. The additional storage often comes in the form of an external hard drive used as the only storage for research data. These drives are rarely backed up and often left entirely unmanaged by an IT professional. Failure, damage, or theft of the external drive would result in a complete loss of the research data on it.

Management Plan - LSA will work with ITS to ensure that cost-effective, reliable, central data storage is available to LSA researchers. A review of current options available from departments, LSA IT, and ITS will be performed to determine if any existing solutions could scale out to the rest of the community. Members of the LSA Joint IT Research Committee are exploring third party options as well.

4. Backups - Much of the research performed at LSA is data intensive. Data loss could ruin projects or cause experiments to have to be redone, costing researchers a great deal of time and

money. Effective backups could effectively prevent such data loss. University Audits noted that no backup strategy was in effect for many of the researchers surveyed. Those utilizing backups were often doing so on their own, using a wide variety of solutions, many of which fail to meet industry best practices for security and reliability. Researchers cited a lack of a centrally provided, affordable, easy to use backup solution to justify implementing their own backup solutions.

Management Plan - The LSA Joint IT Research Committee will work with LSA IT to develop a central data storage solution that can be used by researchers for backup. The Committee will ensure that cost and ease of use are focus points during the development. The Committee will also ensure the new product is sufficiently advertised to the research community.

5. Training and Guidance - Researchers' areas of expertise lie within their particular disciplines. They are not, and should not be expected to be, IT professionals. They are often unaware of IT best practices, security concerns, and the solutions to their computing needs and problems. This lack of knowledge results in the implementation of solutions that may be inefficient or compromise security. University Audits found that many researchers were unaware of current services provided by LSA IT and ITS that would address their research computing needs, resulting in the use of inefficient and sometimes insecure practices, and unprotected research data. LSA IT and department IT teams should work together to provide training to the research community to educate them about the computing services available and data security best practices.

Management Plan - The LSA Joint IT Research Committee will develop a web site containing the suggested information. This site will be regularly reviewed and updated as changes are made to IT infrastructure.

6. Antivirus - University Audits found that some researchers are not using antivirus software on the systems they use to perform research and store research data. Researchers stated that antivirus software slowed their computers to an unacceptable level. Failing to utilize antivirus software puts the individual machine, the data on it, and the systems on the same network as that machine at risk.

Management Plan - LSA IT Security will review current policy and update, if necessary, to include a requirement for antivirus software on Windows and OS X machines. Departmental IT Security Policy should list any exceptions to this policy with justification.

7. Disaster Recovery Plan - An effective disaster recovery plan (DRP) can help an organization such as LSA quickly and effectively resume operations after severe weather, fire, flood, or similar disaster affecting IT resources. A well crafted DRP ensures data is protected, and will be recoverable. Some of the units reviewed for this audit had no disaster recovery plan.

Management Plan - The LSA Joint IT Research Committee will work with LSA IT, departmental IT, and researchers to develop DRPs as needed.

8. Physical Security - Having physical access to a computer removes all of the challenges of connecting to a system through the network. It also eliminates any protections provided by network controls such as firewalls.

The level of physical security for research systems reviewed varied widely. Some departments cited policies requiring staff to lock office doors when they left to prevent physical tampering.

Some departments had no such requirements. Many departments stated that their systems were housed in data centers controlled at the school, college, or University level, and were therefore assumed to be secure.

Each department should decide what level of physical security is appropriate for their research computers and the data they store. Departmental IT should review the security policies and practices for the data centers that house their research servers. In each instance, physical access to hardware containing research data should be restricted to those with a demonstrable and legitimate need for access.

Management Plan - Physical security of IT resources should be addressed within each department's IT Security Plan. The LSA Joint IT Research Committee will work with departmental IT staff to ensure security plans are up-to-date, and physical security is appropriately addressed within them.

University Audits will perform a formal follow-up to the outstanding issues during the second quarter of fiscal year 2011.

University of Michigan Portable Electronic Devices UMHS
Report issued August 26, 2010

#2009-305

Portable electronic devices (PEDs) are defined as any electronic device that is capable of storing user-supplied information and is easily transported. Such devices include portable computers such as laptops and netbooks, handheld devices such as smart phones, PDAs, mobile phones, media players, and storage devices such as thumb drives. Smart phones constitute a significant percentage of PEDs on the UMHS network utilizing Post Office Protocol (POP) server or BlackBerry Enterprise Server (BES) to retrieve email and calendaring events. MCIT management of over 1,200 BlackBerry devices, of which 280 are purchased by MCIT, is the focus of this audit.

Introduction of portable electronic devices into an organization takes place either through purchases by individuals or controlled purchasing and distribution by the organization. UMHS policy "covers all UMHS-owned or managed portable electronic devices...used by UMHS workforce members to store or access sensitive information, regardless of ownership."

This audit included an examination of the processes surrounding configuration, issuance, and use of portable electronic devices (specifically BlackBerry smart phones) by Medical Center Information Technology (MCIT). It focused on the processes in place to ensure that:

- Proper policies and procedures exist to secure portable electronic devices
- Portable electronic devices are securely configured
- Portable electronic devices are used in an appropriate manner
- Adequate processes exist for backup and recovery of data and handling of incidents related to theft, loss or compromise of data on portable electronic devices
- Portable electronic devices are protected against loss, theft, and breakage
- Portable electronic devices are appropriately monitored from issuance to secure disposition

This audit specifically targets controls over smart phones configured and maintained by MCIT, which include Blackberry devices purchased by MCIT, department-provided, and personally-owned devices used for business. This audit does not specifically address controls over thumb drives and laptops beyond a review of the policies and procedures addressing these along with smart phones.

Risk and Control Discussion

- Proper Use Standards - Users are not required to sign a Proper Use/User Agreement related to their use of PEDs. Smart phones have the ability to use multiple email services. They have the capability to allow users to easily reply to and forward emails from one email system to another. This could violate UMHS policy requiring use of GroupWise whenever practical when two or more UMHS staff exchange electronic protected health information (ePHI). Proper Use/User Agreement forms can forewarn users of potential issues related to multiple email accounts configured on a single device.

Raising user awareness through proper use training would greatly minimize the potential of a sensitive email being inadvertently sent via unauthorized means. Before MCIT configures a PED for use with UMHS email client, a User Agreement/Proper Use form should be reviewed and signed by the user.

Management Plan - UMHS agrees with the recommendation to implement a User Agreement specific to the Portable Electronic Devices and will implement a process.

- Exposures Based on Standard Configuration - No password complexity requirements are defined in the standard configuration used by MCIT for Blackberry devices. A password that is trivial and easily guessable can result in unauthorized access to sensitive data on a device that is lost, stolen, or left unattended. Blackberry configuration settings include a parameter that can be used to ensure that strong passwords are set on the device. If configured securely, this parameter will force users to set complex passwords. In order to facilitate the creation of stronger passwords, the 'Password Pattern Checks' configuration parameter should be changed to '2' (from 0).

Management Plan - MCIT will take this recommendation under advisement with the UMHS Compliance Office to identify a plan of action to address this issue.

- MCIT: Mobile Devices Policy - Policy governing security of PEDs within UMHS is addressed by both UMHS Policy 01-04-502 and MCIT Policy 03-006-001. At present, these policies complement each other. However, because the owners of the individual policies are different, changes made to one policy could create conflict between these two policies. For instance, MCIT is changing Policy 03-006-001 so that the policy no longer requires encryption on portable electronic devices. This change will make MCIT less restrictive than UMHS, which still requires encryption on portable electronic devices. This situation would result in a less restrictive policy at the department level than in the organization overall. This conflict is mitigated somewhat because UMHS policy does allow for exceptions of the encryption standard with manager or supervisor approval. MCIT may choose to seek an exception of policy rather than modifying current policy.

Management Plan - MCIT will take this recommendation under advisement with the UMHS Compliance Office to identify a plan of action to address this issue.

- Access Control - To prevent unauthorized access and potential loss, compromise, and/or destruction of information, it is essential that accounts be properly controlled and restricted only to authorized users. Sensitive information within UMHS is potentially vulnerable to unauthorized access and exploitation by individuals using accounts on PED's that should have been deactivated. Accounts of individuals who have transferred from UMHS, had their

employment terminated, or are no longer authorized access to UMHS systems or its information resources need to be inactivated. University Audits personnel witnessed MCIT procedures to identify and remove unauthorized accounts manually from the Blackberry Enterprise Server (BES). These procedures are not documented and rely on MCIT personnel to manually disable and delete the PED accounts.

Management Plan - MCIT agrees with this recommendation to document the procedure for termination of accounts and will document the process as requested. The automation of this process will be evaluated as part of the Exchange project.

University Audits will conduct a follow-up of Management's progress on action plans in the third quarter of fiscal year 2011.

Health System

University of Michigan Medical School W. K. Kellogg Eye Center Business Operations Audit#2010-204
Report issued August 27, 2010

University Audits completed a review of the business operations at the W.K. Kellogg Eye Center (Center), which is part of the University of Michigan Health System (UMHS) and the Medical School. The Center, opened in 1985, houses the Department of Ophthalmology and Visual Sciences clinics, laboratories, and offices. Included are six clinics, four operating rooms, a research tower with fourteen laboratories, an ophthalmic photography service, an optical shop, a library, and faculty offices. In March 2010, the Center opened the Brehm Tower, a 230,000 square foot expansion to further support diabetes and vision research, education, and patient care.

The primary objective of the audit was to review the operational and financial internal control environment at the Center. University Audits evaluated internal control risks in the following areas:

- Financial monitoring and oversight
- Procurement and travel
- Grant management and effort reporting
- Inventory management
- Charge capture
- Payroll
- Cash handling

Risk and Control Discussion

1. Financial Monitoring and Oversight - The Center utilizes various mechanisms for Statement of Activity (SOA) reconciliation and financial oversight. Grant and department administrators, directly familiar with research activities, review expenditures on federal and non-federal grants and faculty professional development accounts. Reviews performed by the Center's Finance Office include review of SOA details for unusual/unexpected transactions and explanations for large purchases. Transactions are not consistently reconciled to source documentation.

Financial monitoring and oversight issues specific to the Optical Shop include:

- Currently, management does not review Optical Shop SOAs. Establishing a robust reconciliation process will assist management in determining the appropriateness of recorded transactions.

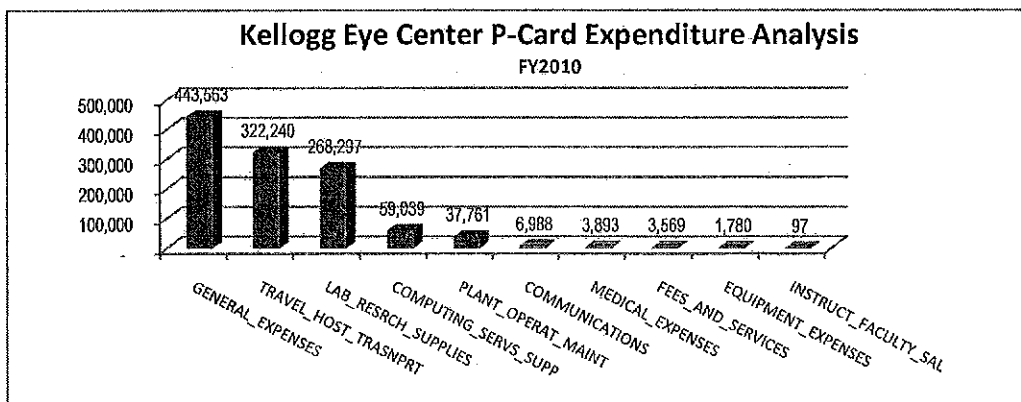
- Bank statements are not reviewed or reconciled against deposits and expenditures. Monthly reviews should include an independent analysis of payments, refunds, and credit card charge backs.
- Someone independent of the sales function should 1) review merchandise forms to ensure all sales orders are recorded and 2) compare actual cash collections with the bank's record of deposit to ensure all collections were deposited intact. Adequate segregation of duties reduces the likelihood that errors (intentional or unintentional) will go undetected.
- Improvements are needed to ensure balances owed on eyewear are collected upon delivery. Most patients pre-pay eyewear orders. At management discretion, a small percentage of patients (five to ten percent) pay upon delivery. An enhanced process for labeling orders that are not pre-paid will ensure staff collects final payments upon delivery.

Management Plan - Department-wide reconciliation procedures will be documented and increases in systematic, detailed tracing of expenditures to the SOAs will be implemented for areas where improvements will be cost-effective.

The Optical Shop will develop adequate segregation of duties including independent review and reconciliation of SOAs and bank statements. Written policies and procedures will be developed including clear processes to identify and collect any unpaid balance on eyewear balances.

2. **Procurement and Travel** - Two Finance Office employees are responsible for reviewing all expense reports (i.e., P-Card Statements, travel and hosting reports). The Chief Department Administrator is responsible for approving them. The approver is attesting that s/he thoroughly reviewed each transaction and supporting documentation, and verified that all transactions are allowable. Currently, the Center has over 350 faculty and staff (75 with active P-Cards) who could potentially submit an expense report during the month. University policy recommends that approvers have responsibility for approving expenses for no more than 25 expense submitters. A review of a sample of transactions indicated opportunities to improve the Center's current review and approval processes. During the audit, several examples of over reimbursements ranging between \$25 and \$500 were noted. The review also indicated a history of late expense report submittals.

Improved cost analysis of P-Card spending may provide additional benefits to the Center. Annual P-Card spending at the Kellogg Eye Center is approximately \$1.1 million. At a summary level, this spending is allocated as follows:



The categories of general expenses and laboratory research supplies comprise more than 60% of the total P-Card spend for fiscal year 2010. Procurement Services recommends departments limit P-Card activity to business travel and hosting expenditures, dues, subscriptions, and other small dollar infrequent transactions. Detailed analysis of these two categories could indicate specific items or groups of items that would cost less through the use of strategic vendor contracts.

Management Plan - The Chief Department Administrator will implement a process, per the recommendation above, to reassign approval responsibilities and develop departmental reconciliation and review procedures. The Chief Department Administrator will also review P-Card expenditures with the Procurement Department to determine if better pricing can be obtained using negotiated contracts.

3. Grant Management and Effort Reporting - Project administrators maintain budgetary information for primary investigators detailing staff effort and other expenditures. The Center's Human Resources Office ensures faculty and staff submit effort certifications. A review of these processes showed that several employees needed to recertify effort for fiscal years 2008 and 2009 because of retroactive changes to payroll budget allocations.

Effort recertification raises several concerns, including insufficient grant monitoring and budgeting processes causing retroactive adjustments, the appearance of effort and expenditure co-mingling between grants, the lack of a robust Human Resources process to follow-up on certifications, and a concern that faculty and staff do not fully understand what they are certifying.

Management Plan - The Center will initiate quarterly reviews of effort with faculty and staff to ensure effort is correct. The Grants Management and Finance Offices will notify the Human Resources Office, in writing, when funding changes related to effort certification take place. They will also copy the Chief Department Administrator on these communications. The Human Resources Director has assumed responsibility for ensuring employees complete recertifications. The Human Resources Director will notify the Chief Department Administrator of any uncompleted recertifications that are outstanding for more than 30 days.

4. Inventory Management - The Center is responsible for a significant level of supply purchases and related inventory. A review of inventory practices revealed the following control risks:
 - Management performs periodic inventory counts in the Optical Shop but does not have a process to reconcile inventory counts to purchase and sales records, which would detect shrinkage and unusual activity.
 - Several high-cost drugs are used in the Retina and Eye Plastics Clinics. The Center's process for ensuring these medications are billed to patient accounts does not include a physical inventory count to reconcile medication remaining on-hand and medication that was removed from the clinic for use at satellite locations.
 - One clinic maintains an inventory of a controlled substance that is used as a topical anesthetic. Clinical staff maintains usage logs and perform periodic inventories to deter misuse. However, key access to the storage location is widely available to clinical staff because the anesthetic is occasionally used after hours. UMHS Pharmacy policy states keys to containers housing controlled substances should be in the possession of a charge nurse (or other designated responsible party) and carried at all times. The key should not be stored or left in an accessible place.

- Credit due for returned items is not tracked and traced to financial statements (or subsequent invoices) to ensure proper credit was obtained from vendors.

Management Plan -

- The Optical Shop is in the process of establishing a perpetual inventory system. The new system will enable management to reconcile purchases to sales records.
- The Center purchases \$4 million per year in injectable pharmaceuticals primarily for the treatment of macular degeneration and muscle spasms, with a modest amount used for cosmetic purposes. The Center has established processes to maintain inventories at low volumes and will modify the current logging process to ensure staff properly account for medication. The Center will also establish an adequate inventory rotation process.
- The Center will work with UMHS Pharmacy to improve access controls for maintaining controlled substances.
- The Center will establish and document procedures to ensure departments track credits for returned and damaged items.

5. Charge Capture Process - The Center has a centralized review process to ensure charges listed on billing documents are entered into the University's billing system. A review of charge posting activities in clinical areas revealed clinical managers do not review Patient Removed from Census Reports to verify the appropriateness of voided billing forms and visits coded as "no charge."

Management Plan - Clinic Coordinators and Community Office Managers will review the Patient Removed from Census Report on a daily basis.

6. Payroll - Faculty and staff salaries and associated fringe benefits account for seventy percent of the Center's expenditures. A review of payroll practices revealed that staff reconciles Gross Pay Registers to source documentation for appointment changes and reviews overtime payments for appropriateness. However, several opportunities to improve payroll practices were noted during the review:

- Time entry validation - Data input (reported in Payable Time Reports) is not verified to approved time data
- Tuition support documentation - The Center does not have a process for ensuring employees who receive tuition assistance submit verification of satisfactory completion of courses
- Segregation of duties - Segregation of duties over timekeeping responsibilities for temporary employees needs to be improved
- Other responsibilities - On two occasions, employees received payouts that exceeded UMHS PTO (paid time off) Buyback Program guidelines

Management Plan - The Chief Department Administrator took the following actions to address payroll concerns raised in the audit.

- Instructed Timekeeper to reconcile data entries to source documentation
- Created a log to track tuition assistance payments and revised review procedures
- Reassigned Gross Pay Register reconciliation of temporary employee payroll to financial staff
- Revised PTO buyback payout practices to include a secondary review to double check calculations

7. Cash Management - Clinic cash handling practices appear adequate. Staff maintains cash, checks, and credit card receipts in secure locations, payments are promptly entered into the charge capture system, credit card machines are closed out at the end of the day, and clinical areas perform daily reconciliations.

A review of change funds revealed inconsistencies with the University's Imprest Cash Funds policy, including two unauthorized change funds, two change funds maintained by someone other than the fund custodians, and no reviews by a higher administrative authority to verify funds are maintained in accordance with University policy.

Management Plan - To more clearly define accountability and separate change funds from revenues, the Center will modify the names of fund custodians for two existing funds and has established \$50 change funds for the Ann Arbor and Canton Optical Shops. The higher administrative authority for the Center's imprest cash funds, or a designee, will periodically audit funds to ensure custodians maintain funds in accordance with University guidelines.

8. Management Structure - Currently, all department managers whose primary responsibilities include the day-to-day operations of the Center report directly to the Center's Chief Department Administrator. In 2009, the Financial Director resigned and the position was not refilled due to budgetary constraints.

The Center should reconsider the reinstatement of this position by appointing a business manager to its management structure to perform financial analyses, oversee training, provide oversight of day-to-day functions, and perform other administrative functions.

Management Plan - In order to reduce administrative overhead, the Chief Department Administrator assumed managerial responsibilities previously performed by the Finance Director and delegated additional responsibilities to Finance Office staff. The lack of a Finance Director left some Finance Office staff unclear about their roles and responsibilities; management has met with staff to clarify job expectations. Team building in the Finance Office is necessary to address concerns regarding levels of authority. As the Center resumes its growth and financial strength, Center Administrators will consider filling this essential position to increase hands-on management of internal control functions and provide support to administrative managers.

Management needs to address control risks in many of the core administrative processes. There is a lack of management resources, including a management position that provides the appropriate level of attention to day-to-day business processes.

University Audits will conduct a follow-up review in the third quarter of fiscal year 2011 to assess the adequacy and effectiveness of corrective actions implemented by management.

Follow-up Reviews

University of Michigan Health System Cardiovascular Center Supply Chain Second Follow-up Review

#2009-105

Original Report issued May 15, 2009

First Follow-up Report issued February 26, 2010

Second Follow-up Report issued August 13, 2010

All remaining corrective action plans have now been completed. **This audit is closed.**

- Blanket Purchase Orders - Blanket purchase orders were routinely used to purchase EP (Electrophysiology) implantable devices from vendors. At the time of the audit, University Audits recommended that CVC discontinue the use of blanket purchase orders and replace them with an inventory and supply chain management system already in use at the health system.

The QSight Inventory Management system is now fully operational with the July 2010 launch of the EP requisition loader; blanket purchase orders for EP implantable devices will be phased out over the next six months. **This issue is closed.**

- EP/Cath Inventory Shrinkage Tracking - University Audits recommended that periodic physical counts of inventory and reconciliation of inventory records should be conducted to monitor inventory. Physical inventories and cycle counts are now performed and the department has developed a monitoring process for inventory adjustments, shrinkage, and aging. **This issue is closed.**
- Supply Chain Policy and Procedures - Within Cath/EP/IR, written, formal procedures for managing the supply chain generally did not exist at the unit level. University Audits recommended that formal written procedures be developed for each unit. The procedures are now fully developed and on the departmental shared drives for employee use. **This issue is closed.**

Southwest Oncology Group (SWOG) Follow-up Review

Original Report issued February 25, 2010

#2010-501

Follow-up Report issued August 18, 2010

University Audits conducted a follow-up review to determine if corrective actions were implemented. Management has satisfactorily completed five of six action plans. University Audits will report on the status of the remaining action plan during the second quarter of fiscal year 2011.

- SWOG Purchase Service Agreement - University Audits' review of pass-through payments to SWOG members identified that a Purchase Service Agreement was missing and the agreement template required updating. Management has obtained the missing agreement and updated the agreement template. **This issue is closed.**
- 1099 Reporting - Payments made to SWOG members via the SWOG accounts payable hub were not included in the University's 1099 tax reporting system. Procurement Services has corrected the problem. **This issue is closed.**
- Employee Time Records - SWOG employee time records were not always approved timely in the Self-Service Timekeeping System. Subsequently, management has approved the overdue time records and developed a process to follow-up on unapproved time records in the system. **This issue is closed.**
- Late Payment of Overtime - Two SWOG employees who worked overtime and whose employment classification required payment of overtime pay were paid the overtime several months late. University Audits did not identify further late payment of overtime during the follow-up review. **This issue is closed.**
- Effort Reporting - All Hematology/Oncology employees' effort has now been certified for fiscal year 2009. Additionally, the Department of Internal Medicine management added effort

certification to the termination checklist to ensure that terminated employees certify effort prior to leaving the department. **This issue is closed.**

- Grant Management - Management has transferred unallowable hosting expenses identified during the audit off the federal grant. University Audits found no indication of other unapproved or prohibited expenses charged to federal grants during the follow-up review. **This issue is closed.**
- Statements of Activity Reconciliation - Statements of Activity reconciliations are not up-to-date due to short-term personnel constraints. University Audits will follow-up on management's progress in addressing this issue during a second follow-up review in December 2010.

Center for Human Growth and Development
Original Report issued November 17, 2009

#2009-206
Follow-up Report issued August 26, 2010

Management has taken corrective action on some audit recommendations and made progress on others as outlined below. University Audits will follow-up again in the third quarter of fiscal year 2011.

- Security/Maintenance of Sensitive Data - To improve management of sensitive information, PEERRS training (The U-M's Program for Education and Evaluation in Responsible Research and Scholarship), which includes a section on privacy and confidentiality, is now required for administrative staff at CHGD. The Human Subjects Incentive Program payment system is used for all of CHGD's research projects. Staff has begun the process of cleaning out electronic and hard copy files to ensure only necessary information is maintained and sensitive data is adequately secured.

During the next follow-up, University Audits will:

- Review CHGD's documented business process for managing sensitive information
- Confirm staff have completed PEERRS training

- Monitoring Grant Budgets - Since the audit, CHGD has used both their supplemental system and MReports to provide budget reports to Principal Investigators on an as-needed basis. A new position was recently filled to help administer and monitor grants. CHGD still plans to consult with Information Technology Services (ITS) to determine if reporting needs can be met efficiently and effectively using U-M systems.

During the next follow-up, University Audits will:

- Confirm CHGD completed an analysis of their current supplemental system, working with ITS, to determine the best method for providing faculty with reports to monitor their budgets on a regular basis.
- Review documented procedures for the budget monitoring process, including maintenance of the supplemental system, if necessary.

- Disaster Recovery/Business Continuity Planning - ITS conducted a vulnerability scan for CHGD which identified a few vulnerabilities that CHGD is in the process of eliminating. CHGD's IT Manager plans to meet with each researcher to assess what critical data is maintained at their site and understand the impact of various disasters. The IT Manager and Assistant Director will then work with the researchers to ensure all sensitive/important research data is secure.

During the next follow-up, University Audits will:

- Review the results and actions taken as a result of the assessments of research data maintained onsite.
- Obtain an update on the status of expanding the business continuity plan to address various threats to CHGD's continuity of operations.
- Statement of Activity (SOA) Reconciliation/Segregation of Duties - The recently hired grants and contracts administrator will reconcile the SOAs for grants. This individual does not have system access to control a transaction from start to finish. For the general fund, the Financial Specialist obtains the support documentation for transactions and the Assistant Director completes the reconciliation. Both of these individuals have procurement access but they serve as checks for one another. CHGD plans to start using eReconciliation. Adding and removing system access is now included on CHGD's new employee and termination checklists.

During the next follow-up, University Audits will:

- Review the new process for reconciling SOA's using eReconciliation.
- Procurement Process - The Office of the Vice President for Research (OVPR) now approves large transactions made by or on behalf of the Director. OVPR plans to document this requirement for all its units, including guidance on the types of transactions that may require prior approval.

During the next follow-up, University Audits will:

- Review the documented procedures for approving the Director's expenses.
- Confirm appropriate approval for a sample of expenses.
- Payroll - To help reduce the risk of inaccuracies or inefficiencies in time reporting for staff reporting to faculty, CHGD developed a cover letter, which is sent every two weeks with the time reports, that must be signed by the approver. By signing the cover letter, the approver is attesting that either they are aware of the hours worked and the timesheets are correct or they can compare the reported hours to productivity thereby confirming the accuracy. The majority of CHGD's retroactive payroll adjustments for fiscal year 2010 were made in less than 60 days from when the need for adjustment was identified. Within the next few months, CHGD plans to use eReconciliation for completing and documenting GPR reconciliations. **This issue is closed.**
- Registration with ITOC - Insurance Requirements - Faculty and staff were reminded of the requirement to ensure that all international travel was registered with the U-M's International Travel Oversight Committee (ITOC). CHGD is in the process of procuring a vendor to redesign their public website and develop an internal website for CHGD personnel. A link to the ITOC website and the requirement to register will be included on the internal website with other helpful travel information.

During the next follow-up, University Audits will:

- Confirm CHGD's website has been updated with international travel registration information.
- Evaluate procedures for making sure staff is aware of and following current practices relevant to international travel.
- Documented Procedures - CHGD is continuing to work on documenting business processes. As part of the staff re-organization, key processes were identified and assigned to individuals, which

will help with documenting procedures. New employee and termination checklists are now documented.

During the next follow-up, University Audits will:

- o Review progress made toward documenting key business processes.

UM-Dearborn Grade Changes

Original Report issued November 5, 2001

#2009-109

Follow-up Report issued August 26, 2010

Management has taken appropriate corrective action on all audit recommendations and improved internal controls as detailed below. **This audit is closed.**

- Faculty Grade Change Notification - The Office of Registration and Records (ORR) was mailing the instructor's copy of a completed grade change to the unit administrative office via campus mail. This practice does not ensure notice to the faculty of grade changes independent of staff in the administrative unit who could also initiate a grade change request.

The instructor's copy of a grade change request is now mailed directly to the faculty member's office in a sealed envelope. ORR is investigating mechanisms for delivering this information electronically.

- Access to Supplemental Grade Reports and the Grade Change System - Supplemental Grade Reports (SGR) used to authorize grade changes were stored in an unlocked file cabinet in ORR. Approximately 20 staff members had access to the forms, including individuals with access to the Banner System Term Course Maintenance screens used for making grade changes.

SGRs are now kept in a locked filing cabinet in a locked storage room. Access is limited to Administrative Officers and Enrollment Services Associates (ESA). None of these individuals have access rights to the grade change screens in Banner. A log is updated as forms are distributed. The log is also kept in the locked cabinet and is reviewed monthly for anomalies by the ESA supervisor.

- Management Review of System Access Reports - During the audit, testing showed that four individuals had inappropriate access to the Banner grade change screens. Three ORR staff also had improper access to the Oracle tables that contain grade change data. Procedures for requesting and confirming changes to access rights were not comprehensive.

Management reviewed access reports and requested and confirmed termination or restriction of access rights for six employees. ORR developed a form for requesting and verifying changes to access. Management now reviews grade table activity logs on a quarterly basis to verify appropriate access to the tables. ORR is working with Information Technology Services to eliminate the need for ORR staff to have access to any Oracle tables, further strengthening controls.

- Registration and Records Policy and Procedures - Although ORR could describe their grade change process verbally, documented policy and procedure did not exist.

Management developed a comprehensive guide for processing supplementary grade reports. The guide addresses the campus grade change policy and documents procedures for employees in both ORR and the academic units.

- Baseline Controls in Units - Audit interviews indicated a high degree of variance in controls within grade change procedures among academic units.

Management developed baseline controls guidance and included it the procedural guidelines referenced above. Some of controls established for academic units include:

- Securing and logging distribution of grade change forms.
- Requiring identification before releasing forms to unknown individuals.

University Housing Fiscal Responsibilities

Original Report issued November 9, 2009

#2009-814

Follow-up Report issued August 26, 2010

Detailed information regarding progress by management on corrective actions is below. University Audits will conduct a second follow-up in second quarter of fiscal year 2011 to assess the remaining items and in some cases to assess that recent improvements are working as intended.

- Centralized Business Processes - University Housing's (Housing's) central purchasing, payroll, and billing offices were located in numerous buildings across campus. A number of smaller offices with similar responsibilities existed within a number of departments.

Housing, working with University Human Resources, developed and implemented a reorganization of the Housing Business and Finance area with the goal of improving management oversight and more effectively coordinating processes and procedures. Realignment of both staffing and office locations were aimed at streamlining workflow and strengthening financial internal controls. Management has already experienced an improvement in the accuracy and flow of information as a result. The Director of Housing Business and Finance will continue to monitor the effects of the reorganization and make adjustments where necessary. **This item is closed.**

- Purchasing Management - Internal controls around Housing's purchasing activities needed to be strengthened in many areas. Management responded to audit recommendations quickly and have made good progress. Actions taken include:
 - Reorganization of Housing Business and Finance purchasing roles and responsibilities as part of the restructuring of that area. A new purchasing supervisor was hired to oversee inventory practices and spend on items such as supplies, furniture, and equipment. Training related to purchasing best practices, specifically the proper use of M-marketsite, is under development. Management is investigating opportunities to strengthen controls around vendor use within Housing facilities.
 - Signature authority for journal entry, P-Card statement, and travel and hosting approval has been limited to the Housing leadership team.
 - P-Card holders have been reduced by 40% and gift cards are no longer used.
 - Centralization of the remote business offices in the Student Activities Building and South Quad has strengthened segregation of duties in these areas. Management is working to identify ways to improve separation of duties within the facilities areas, specifically related to project management and work with outside contractors.
 - The Director of Housing Business and Finance is now responsible for the Housing fleet. A deliberate reduction of the vehicle inventory is underway. As leases expire on vehicles, they are not renewed or replaced. Departments that lose vehicles through this process have to justify the need for a vehicle and, based on that information, will likely

be required to share a vehicle with another department. Housing has started requiring the use of vehicle logs to track mileage and frequency of use to facilitate analysis.

- Management is working with Plant Operations to transition to the FMAX Asset Management module. Housing began using the FMAX Purchasing and Inventory modules in July 2010 and has seen improvements in their ability to identify and strengthen procedural weaknesses.

University Audits will review management's progress towards strengthening segregation of duties within Housing Facilities area, specifically related to vendor use and project management along with any other remaining corrective actions during the next follow-up review.

- Standardized Policy and Procedure - Housing lacked a comprehensive and easily accessible repository of standardized policies and procedures.

The Division of Student Affairs (DSA) is in the process of developing policies and procedures templates in accordance with University guidelines. DSA will be able to customize these templates to a degree to accommodate business processes unique to each unit. The Director of Housing's business offices is a member of the division-level committee charged with creating these documents and can provide input into the process on behalf of Housing.

- Comprehensive Financial Reporting and Analysis - Housing management was not receiving adequate information to support business decisions. The use of financial shadow systems and different reporting formats prevented automated roll-up of transactional data across the unit. Manual oversight reports were cumbersome and ad hoc analysis was nonexistent.

Housing's Director of Business and Finance is working with leadership to identify reporting and analysis needs. Redesign of unit core reporting structures and standardization of revenue and expense categories is in progress. Development of financial oversight reports is under way and reports will continue to be refined as planned improvements to the unit's accounting structure are implemented. In the interim, M-Reports and Business Objects predefined reports are reviewed monthly. Examples include:

- Vendor Utilization for Department or Department Group
- Staff Earnings by Department Group
- Pay Temporary Analysis for Funding Department or Department Group

During the follow-up review, University Audits observed Housing's ability to analyze enterprise data quickly and efficiently in response to a possible conflict of interest. **This item is closed.**

- Discretionary Funds - The intended purpose of Housing's discretionary funds, primarily the Student Operations Reserve Fund, was not clearly defined. Access to funds was not appropriately limited and no formal process existed for requesting and approving disbursements.

Housing has defined and documented the intended use of their Student Operations Reserve Fund as funding for large-scale renovation and renewal projects and priority deferred maintenance needs. Housing's Business and Finance and Facilities staff have worked together to develop a project request process that requires review and approval by Housing leadership prior to the initiation of any project. Housing estimates that over one million dollars in requests that would have been automatically approved in the prior funding model have been rejected due to lack of substantiated need during fiscal year 2010. **This item is closed.**

- Payroll and Time Reporting - Supervisors did not have knowledge of actual time worked and some employees were claiming large amounts of overtime while receiving little or no oversight. Management of temporary appointments was problematic in that some part-time staff were asked to work full-time schedules. During the audit, Housing issued a suspension on overtime as a temporary stop gap.

The Housing Payroll Office now reports to the Director of Housing's Human Resource Office. The Manager of Payroll is assisting with ongoing analysis of part-time and temporary staff workloads to ensure part-time staff are not asked to work full-time schedules without the associated benefits. Management is also working with supervisors, particularly in the trades area, to better utilize regular internal staff to maximize efficiency and minimize cost related to contracting outside vendors or temporary employees to complete projects. Procedures for utilizing Housing's electronic timekeeping system have been developed and policies related to overtime, scheduling, and time reporting are under review. Progress in this area will be reviewed during the next follow-up review.

- Management of Cash Operations - Housing was paying the Michigan Union's business office to manage most of the cash handling for their retail operations. Strength of internal controls varied widely by retail operation as did policy and procedure.

Management of cash handling for Housing's retail operations has been transferred to Housing's Billing Office, representing a significant cost savings. Housing has completed their cash handling gap analysis with assistance from the Treasurer's Office and identified internal control weaknesses are being addressed. Examples of controls implemented to-date include:

- Development and distribution of a standard daily sales and deposit log for use by all retail operations.
- Addition of cash drawers, where necessary, to ensure only one person has access to and is solely responsible for each drawer.
- Implementation of annual training on cash handling, reconciliation, depositing, and reporting.
- Daily review of sales and deposit information for all cash operations by Housing's Billing Office.
- Development of performance metrics and standards.

Housing has made substantial progress toward strengthening their cash handling controls. During the next follow-up, University Audits will verify the newly implemented procedures are working effectively.

- Comprehensive Internal Control Gap Analysis - Housing had not completed any of the gap analyses developed to assist departments with identifying internal controls gaps as part of the annual financial certification effort.

Although Housing has completed a gap analysis on cash handling to help guide the development of policies and procedures around cash operations, further efforts hinge on DSA's development of standardized internal control gap analyses templates for the Division.

- Travel and Hosting Management - Housing did not have a uniform travel and hosting policy. Departments within Housing developed their own policies making it difficult to monitor and enforce compliance.

DSA implemented a new division-wide travel and hosting policy in January 2010. The policy is compliant and in some ways more restrictive than University guidelines, and specifically addresses the need for original receipts as appropriate. Housing provided training to personnel based on DSA guidelines and emphasized that exceptions to DSA policy must be approved in advance by the Director of Housing or a higher authority in DSA. **This issue is closed.**

- Fundraising and Gift Management - Housing does not have the requisite gift management and fundraising experience to appropriately steward and increase gift revenue.

Housing leadership is working with the new Student Affairs Development Officer to identify fundraising opportunities and develop strategies. The Housing Business and Finance Director is in the process of developing funding plans for Housing endowment distributions to ensure the proper and efficient use of existing balances and future distributions.

- Business Continuity and Disaster Recovery Plans - Prior to the audit, Housing self-identified many crucial business processes and developed disaster preparedness and continuity plans for these processes. However, the plans were incomplete and had not been tested.

Management is working with Occupational Safety and Environmental Health to ensure plans are comprehensive, up-to-date, and tested as appropriate. Progress will be reviewed during the next follow-up.

- Conflict of Interest/Commitment - Housing implementation of DSA's COI/COC policy did not extend beyond staff with procurement responsibilities.

The DSA COI/COC policy is currently being rolled-out to all Housing staff as part of the annual performance evaluation process. Management plans will be promptly developed for all disclosures made by staff. Review of the COI/COC policy will also be added to new employee orientation procedures. University Audits will review the results of the unit-wide policy roll-out during the next follow-up review and specifically verify that staff have a clear understanding of what constitutes a conflict of interest or commitment.

Wire and ACH Transfer Process

#2009-112

Original Report issued January 6, 2010

Follow-up Report issued August 27, 2010

Management has taken appropriate actions on most audit recommendations. Some of the risks identified during the audit are being addressed through the implementation of a new wire transfer process. A summary of this process is included below. A few items are still in progress. University Audits will conduct a second follow-up review during the second quarter of fiscal year 2011 to reassess the status of these outstanding items.

- New Wire Transfer Process - The Fiscal Collaboration Team, a group with representatives from the Treasurer's Office, Procurement and Accounts Payable, Financial Operations, and Information Technology Services, has developed a new wire transfer process. According to this process, the Vendor Payment Form is integrated with the payment voucher and is completed in M-Pathways by the end user. This reduces paper flow of documentation and improves efficiency by eliminating duplicate data entry for wire and ACH transfers. The voucher goes through the regular approvals at the department and Accounts Payable level in accordance with University procurement policies. The new process improves the electronic vendor payment process for international wires or drafts. A daily file of wire transfer payment requests is

uploaded in Custom House's online portal, thus eliminating the risk of sensitive information exposure via email. The new process also provides for better audit trails in M-Pathways. Enhancements to the wire and ACH transfer process are in the pilot phase and are planned to be implemented for the entire campus in October 2010.

Following is a summary of the status of corrective actions taken by management to address concerns raised during the audit.

1. Security of Sensitive Vendor Data - With the new process, payment requests are no longer sent to Custom House via email. A daily query creates a file that is uploaded in the Custom House's online portal through a secure connection. **This issue is closed.**
2. Compliance with Office of Foreign Assets Control (OFAC) Regulations - The Vendor Maintenance team within Procurement Services verifies that new vendors are not listed on the OFAC or Office of Inspector General lists before they are entered in the University vendor table. **This issue is closed.**
3. Strategic Vendor Payment Processing - A team within Procurement Services is working to move all vendors outside of eBilling. Most of these vendors will be moved to eSettlement; some will be transitioned to other invoicing methods such as hard copy invoices. This is a long-term project because it involves contract renegotiations with vendors that can stretch over several months and sometimes even longer. In addition, significant time and resources are needed to ensure the proper IT infrastructure is in place for electronic submission of invoices. Some vendors with whom the University has a significant number of transactions or dollar amounts are already moved out of eBilling, thus reducing the risk of using this system. Additional controls have been incorporated into eBilling in the interim, such as better password protection and data backup. Work on this item is still ongoing. Management has made significant progress and has demonstrated a clear plan for moving vendors out of the eBilling databases. **This issue is closed.**
4. Unallocated Fund Management - Financial Operations uses an unallocated fund for incoming transfers and deposits missing proper account codes to indicate receiving unit. A policy and corresponding procedures to administer this fund has been developed and properly documented. Accordingly, at fiscal year-end 2010, Financial Operations wrote-off the unidentified wire transfers into the designated fund for the Internal Bank Group. **This issue is closed.**
5. Authorized User List - The Treasurer's Office has implemented a procedure to review the list of individuals with access to the Custom House online reporting system and transactional authorization on an annual basis. Finance Human Resources is working on developing comprehensive employee on-boarding and off-boarding checklists for all the Finance units, including the Treasurer's Office. In the meantime, Treasury will develop a list of access rights and privileges to the banking systems to assist with hiring and termination procedures. University Audits will inquire about progress made on the checklist during the second follow-up review.
6. Transaction Limits - Within the new wire transfer process, a Treasury employee has to upload a file with daily wire transfers into the Custom House's online platform. During the planning and pilot phases of the project, management has been investigating ways to either eliminate the need for manual file upload or to ensure no modifications have been

made to the file during transmission. These procedures depend in part on the IT infrastructure that Custom House has in place. If such procedures are not feasible, the Treasurer's Office will implement compensating controls. Accordingly, an independent person in Treasury will double check that no edits have been made to the file sent to Custom House. If either of the aforementioned controls are in place, a call-back process will not be necessary.

The Treasurer's Office looked into setting transactional limits for wire and ACH transfers through Bank of America. For recurring payments, Bank of America's online platform does not provide the capability to set transaction limits by vendor. Setting limits by employee would create a blanket limit for all recurring wire transfers. This process would be counterproductive as it would require secondary approvals on many pre-approved templates for recurring wires. Current controls include:

- Secondary approval is required on non-repetitive transactions.
- Secondary approval is required to set up templates for recurring transactions.
- Other than the dollar amount field, all vendor data in the template is non-editable without secondary approval.
- Repetitive transactions are limited to well-established vendors such as Fidelity and Blue Cross Blue Shield.

These detective controls provide reasonable assurance that inappropriate or inaccurate transfers would be identified. The Treasurer's Office will consider keeping a list of items that are not provided by the University's banking partners. These may be periodically sent to the vendors or considered during contract negotiations. University Audits will reassess the status of the wire transfer process with Custom House during the second follow-up review.

7. Wire Transfer Policy - The new wire transfer process provides better audit trails in the system indicating who initiates, processes, and approves a transaction. End users are provided some information regarding payment terms. However, clearer and more explicit guidelines should be provided for the end users regarding timeliness of wire transfer requests. University Audits will assess the status of this item during the second follow-up review.
8. Controls over Wire and ACH Transfer Process - Banking Services has updated their procedures for reconciling outgoing wire and ACH transfers. The Treasurer's Office is working on developing a comprehensive document that will detail controls, roles, and responsibilities over fund transfers. User access will be reviewed as part of this process. University Audits will reassess the status of this item during the second follow up review. We will also inquire about the progress in updating the Banking Services employee off-boarding checklist.

Open Audits Follow-up Table
August 31, 2010

Audit Title	Report Date	Issues	Expected Completion
Information Technology Central Services 2009-838	12/02/09	Inventory management; billing for services; monitoring services quality and demand; financial monitoring; human resources processes; facilities; procurement	First Follow-up June 2010
			December 2010
Wire and ACH Transfer Process 2009-112	1/06/10	Authorized user list; transaction limits; wire transfer policy	First Follow-up August 2010
			December 2010
University of Michigan Video Surveillance Systems 2009-311	4/14/10	Network connectivity; unnecessary ports, services, and shares; video quality; video handling; video storage; process documentation; cross-training	September 2010
Dearborn Office of Cashiers/Student Accounts TouchNet 2010-303	6/3/10	Application hosting; application vulnerabilities; change control; user roles	November 2010
Medical Center Information Technology Michigan PGIP Analytics Collaborative 2010-302	7/16/10	Risk assessment of local data workspace; project governance; time limit for reporting breaches; control of data use/access disclosure	March 2011
College of Literature, Science & the Arts Research Computing 2010-809	7/26/10	Security policy; data classification; data storage; backups; training and guidance; antivirus; disaster recovery plan; physical security	December 2010
Portable Electronic Devices UMHS 2009-305	8/26/10	Proper use standards; standard configurations; mobile devices policy; access control	March 2011
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
			September 2010
UMHHC Payroll and Timekeeping 2008-110	1/30/09	Human Resource Management System access; systematic data integrity	First Follow-up February 2010
			August 2010
Medical School Administrative Internal Control Review 2008-208	1/30/09	IT strategic planning; reconciliations; gift fund usage; IT security; fire drill regulations	August 2010
University of Michigan Health System Office of the Executive Vice President for Medical Affairs Operational Review 2009-205	11/17/09	Procurement and payroll training; excluded costs; segregation of duties; reconciliations	December 2010

University of Michigan Medical School Internal Medicine, Division of Hematology/Oncology Southwest Oncology Group Review 2010-501	11/25/10	Retroactive grant adjustments; detailed financial reconciliations; late submission of timesheets; up-to-date effort certifications	First Follow-up August 2010
			December 2010
University of Michigan Medical School Michigan Institute for Clinical Research and Health Research Grant Management 2009-106	11/30/09	Non-certified effort reporting; grant adjustments; Veterans Administration Hospital appointments; expense classification; compliance with P-card Guidelines; business continuity plans	September 2010
U-M Hospitals and Health Centers Omniceil Pharmaceutical Distribution System 2010-305	6/16/10	User access; discrepancy reporting and escalation; patient charges; controlled substance procedures	December 2010
U-M Medical School W.K. Kellogg Eye Center 2010-204	8/30/10	Financial monitoring and oversight; procurement and travel; grant management and effort reporting; inventory management; charge capture; payroll; cash management; management structure	March 2011
William L. Clements Library 2008-212	1/26/09	Grant compliance; endowment agreements; collection management; insurance coverage; physical safety and security; reconciliations; recharge rates	September 2010
University Press Inventory and Receivables 2008-203	1/30/09	Accounts receivable; inventory (U-Press continues to implement internal controls in many areas, including those noted in the audit report)	October 2010
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 (Follow-up review will be conducted after the new chair is named)	October 2010
University Housing Fiscal Responsibilities 2009-814	11/9/09	purchasing; payroll and time reporting, cash operations, internal control gap analysis, business continuity and disaster recovery plans, conflict of interest/conflict of commitment	First Follow-up August 2010
			December 2010

Center for Human Growth and Development 2009-206	11/17/09	Security/maintenance of sensitive data; monitoring grant budgets; imprest cash fund management/subject fee payments; disaster recovery/business continuity planning; statement of activity reconciliation/segregation of duties	First Follow-up August 2010
			March 2011
School of Art & Design 2009-201	12/08/09	International programs; supplemental system; statement of activities reconciliation; P-cards; payroll; cash handling	First Follow-up June 2010
			December 2010
International Programs Student Safety Preparedness 2009-111	3/15/10	Coordination of effort; International Travel Oversight Committee travel registry; health insurance; oversight for student-designed programs; individual program evaluations	December 2010
University of Michigan Dearborn School of Education 2010-205	4/26/10	Agreements with external entities; IT risk assessment; documentation for purchase exceptions; conflict of interest contact information	September 2010
Matthaei Botanical Gardens and Nichols Arboretum 2010-202	4/29/10	Safety and security; cash handling; procurement; inventory; community programs;	December 2010
Office of University Development Life Income Gifts Program 2010-806	6/11/10	Unit roles, sharing information, procedural efficiencies, and system opportunities	March 2011
School of Social Work 2010-813	6/18/10	Stewardship of gift funds, segregation of duties, signature authority, policies/procedures, inventory management, relationships with central service units, supplemental systems	February 2011
University of Michigan Center for Statistical Consultation and Research (CSCAR) 2010-809	6/23/10	Recharge rates and workshop fees, segregation of duties, reconciliations, supplemental systems, policies/procedures	March 2011
Center for AfroAmerican and African Studies 2010-820	6/25/10	Significant oversight and other control activities need to be implemented into many processes	December 2010
Intercollegiate Athletics NCAA Compliance Review 2010-401	6/28/10	Complimentary tickets to high school coaches	October 2010
PeoplePay 2010-107	7/16/10	Payroll Office review office; clarification of PeoplePay capabilities; change management	April 2011
U-M Flint Early Childhood Development Center 2010-118	7/19/10	Financial decision-making; Kid's Care system; Web camera access; transportation agreements; imprest cash and snack station fund	December 2010

U-M Flint School of Education and Human Services Fiscal Responsibilities 2010-812	7/19/10	Financial reporting and budget monitoring; segregation of duties; faculty release time; conflict of interest and conflict of commitment; documented policies and procedures	February 2011
---	---------	---	---------------