MEMORANDUM

TO: Todd A. Leach  
Vice President & Chief Information Officer, Information Services

FROM: Kimberly K. Hagara, CPA, CIA, CISA, CRMA  
Associate Vice President, Audit Services

DATE: November 6, 2014

SUBJECT: Mobile Device Management Solution Implementation Review  
Engagement Number 2014-027

Attached is the final audit report regarding the Post Implementation Review of the Mobile Device Management System. This audit will be presented at the next Institutional Audit Committee meeting.

Additionally, please find attached Audit Services audit recommendation follow up policy. Each of the recommendations is classified by type at the end of its identifying number: Significant (S), Risk Mitigation (R), or Process Improvement (P). As you will note in the policy, the classification of the recommendation determines the frequency of our follow up. All follow up results are reported quarterly to the Institutional Audit Committee.

Thank you for your cooperation and assistance during the course of this review. If you have any questions or comments regarding the audit or the follow-up process, please feel free to contact me at (409) 747-3277.

Attachment(s)

c: Cheryl A. Sadro  
Carolee A. King  
Emma L. Ramos  
Robert V. Shaffer
The University of Texas Medical Branch
Audit Services

Audit Report
Mobile Device Management Solution Implementation Review
Engagement Number 2014-027
November 2014

The University of Texas Medical Branch
Audit Services
301 University Boulevard, Suite 4.100
Galveston, Texas 77555-0150
Mobile Device Management Solution Implementation Review
Engagement Number 2014-027

Background
The increasing reliance on mobile devices in an enterprise charged with maintaining the confidentiality of protected information and the integrity of its business networks has required the consideration of new security strategies and new tools. As part of its multi-phased process for expanding the needs of encryption, in October 2012 The University of Texas System (UT System) issued a Request for Proposal (RFP) for selection of a Preferred Supplier of a Mobile Device Management (MDM) solution. Having selected AirWatch, a Preferred Supplier Agreement with UT System and its participating institutions was executed July 15, 2013.

The AirWatch MDM solution supports the management of the institution's data and network security, network services, and software/hardware across multiple operating systems including the Apple (iOS), Windows, Blackberry, and Android platforms. Since September 2013, UTMB Health has implemented a small number of use cases as an evaluation and testing pilot before it begins a full implementation across the organization. Focus of the pilot project includes: Stratus iPad video application for language interpretation services, Voalte One smartphone application for secured caregiver communications, and Epic Rover iPhone application providing secured access to Epic's electronic health record. Although UTMB Health's Information Services completion of an institution-wide implementation is pending, this MDM solution will be used to manage both institutionally and personally owned smart phones and tablets connecting to the UTMB Health network in an effort to optimize the functionality and security of the mobile computing and communications environment while minimizing cost and downtime.

Audit Objectives
The primary audit objective is to determine whether project goals and objectives for the implementation of the new Mobile Device Management solution have been achieved.

Scope of Work and Methodology
Our scope of work included an assessment of pilot project success, in particular, the extent to which the various use cases met their objectives, delivered planned levels of benefit, and addressed the specific requirements as originally defined. Additionally, the scope including identifying lessons learned from the pilot use cases to improve the pending institutional production implementation.

The audit methodology included documentation reviews of business requirements, strategic and tactical plans, scope of work, request for proposal, preferred supplier agreement, institutional participation agreement, meeting minutes and approvals, project request and overviews, implementation methodology, enterprise mobility management configuration framework, product evaluation and testing, price schedules, license requests, communication plan and user guidance, UTMB Health policies and practice standards, and applicable guidance provided by governing organizations. Additionally, we interviewed a broad group of key stakeholders, including UTMB Health business operations and technical support. Supplementing this feedback, we
Mobile Device Management Solution Implementation Review  
Engagement Number 2014-027

benchmarked best practices with the University of Texas Health Science Center at San Antonio, the University of Texas Health Science Center at Tyler, the University of Iowa Health Care, the Medical University of South Carolina, the State University of New York Downstate Medical Center, and the University of Texas-Pan American.

The audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* as promulgated by the Institute of Internal Auditors.

**Audit Results**

**Regulatory Compliance**

A number of regulatory and oversight organizations have requirements to be considered in planning, selecting, funding, controlling, evaluating, and implementing major information technology (IT) initiatives. The Texas Administrative Code 216 (TAC 216) Project Management Practices requires, at a minimum, institutions of higher education approve and publish operating procedures identifying project components and the general use of project management practices. Based on our review, UTMB Health project management practices are in alignment with TAC 216 specifications.

The Texas Department of Information Resources publishes the Texas Project Delivery Framework Handbook (Framework) to provide the state with a consistent statewide methodology for project selection, control, and evaluation based on alignment with business goals and objectives. UTMB Health generally complies with the spirit of the Framework and its supporting documents.

Additionally, The University of Texas System (UT System) developed Policy UTS 140 Enhancing Major Software Projects, which cites the inclusion of various project planning and implementation core elements. UTMB Health's operating procedure(s) "Information Services' Standardized Project Management Process" and UTMB Health Practice Standard "20.20.1.1 Project Management" collectively capture relevant core elements of this guidance.

**Strategic Alignment**

All IT projects are essentially business projects and should have a business rationale from inception; therefore, contribution to the achievement of the strategic business plan influences project success. The UTMB Health IT Governance process design typically advances an IT proposal from initial conceptualization through needs assessment and concept review, alignment with institutional strategic plans, available funding sources, and ultimately executive approval.

Available MDM solution project documentation substantiated the UT System RFP process provided qualifications for the initiation of system development. The subsequent review and approval process of the AirWatch proposal demonstrates the product was determined to meet existing business requirements. Additionally, UTMB
Mobile Device Management Solution Implementation Review
Engagement Number 2014-027

Health’s Information Technology Strategic Plan contains explicit strategies and objectives language supporting implementation of the new MDM solution.

In conjunction with the strategic multi-phased UT System-wide mobile computing and communications security initiative, institutional participation was initially evaluated and approved by UTMB Health’s Institutional Security and Privacy Compliance Committee. UTMB Health’s Executive Institutional Compliance Committee provided final authorization to implement the UT System selected MDM solution with basic institutional capabilities. As determined by UTMB Health’s leadership, the AirWatch MDM solution sufficiently aligns IT investments with institutional needs, priorities, and resources.

Project Quality
Continuous project assessment increases the likelihood that a project will implement a quality solution meeting the schedule, cost, and scope commitments provided to leadership. All IT projects, regardless of size and scope, are expected to be managed using UTMB Health’s standardized project management process; however, the intent of this process is to ensure the effective and efficient use of resources and the achievement of expected outcomes for “major” projects. Categorically, “major” projects include substantial enterprise mission critical software involving highly integrated customer processes which would typically exclude a small pilot project such as the AirWatch use cases. While required for “major” projects, elements such as project charter, budget, and timeline were not formally developed for the AirWatch pilot. We noted the present standardized project management process does not have defined requirements for those projects not classified as “major”. Additionally, MyUTMB, the centralized project/service request tracking system, does not clearly denote a clear exit or transition from the AirWatch evaluation and testing pilot to an institutional production implementation.

Recommendation 2014-027-01-P:
Information Services should revisit the standardized project management process and consider scalability for those projects not involving substantial enterprise systems, and project tracking for phased implementations.

Management’s Response: Information Services will revisit the standardized project management process for scalability of projects not involving substantial enterprise systems and proper project tracking for phased implementations.

Implementation Date: May 1, 2015

Service Performance
Information technology projects initiated by the institution must ultimately have a positive impact on business outcomes. Business goals and objectives outlined in the request for proposal, scope of work, preferred supplier agreement, project request and overviews, and enterprise mobility management configuration framework were as
Mobile Device Management Solution Implementation Review
Engagement Number 2014-027

follows:

- Provide network connectivity to a wide range of mobile device platforms with the ability to manage both institutionally and personally owned devices
- Robust control of the mobile computing and communications environment with improved data and network security capabilities centrally managed by a single system
- Minimized cost/pricing (as an institutional participant in the preferred supplier agreement, product use largely funded by UT System)

Key stakeholders, representing both technical and operational involvement in the pilot use cases, provided their perspective. Based on cross-functional institutional feedback, the pilot project met the stated functional goals and objectives with key stakeholders indicating satisfaction with the new Mobile Device Management solution, AirWatch.

As Information Services prepares to transition the project from pilot to production, additional validations were specifically requested as follows:

- State of the mobile device registration/enrollment process for AirWatch
- State of supporting policy or practice standards to reflect the use of AirWatch
- Comparable AirWatch controls have been transitioned from the existing system, Microsoft’s ActiveSync
- Planned vetting and approval process for future enhancements and maturation of AirWatch

Although the UTMB Health Portable Computing practice standard, last revised September 2013, makes no specific reference to a required device enrollment or registration process, the draft communication plan for institutional implementation articulates a mobile device registration/enrollment process and the availability of a user guidance website. Additionally, we noted the UTMB Health Platform Hardening practice standard, as referenced in the Portable Computing practice standard, and last revised July 2009, is dated and makes no mention of SMART phones or tablets when citing examples of mobile technologies (e.g., laptop, PDA, flash drive).

**Recommendation 2014-027-02-P:**
The Office of Information Security should prepare additions or revisions to the MDM Solution related practice standards as deemed appropriate to reflect a current state of operations.

**Management’s Response:** The Office of Information Security will prepare additions or revisions to the MDM Solution related practice standards as deemed appropriate to reflect a current state of operations.
Mobile Device Management Solution Implementation Review
Engagement Number 2014-027

Implementation Date: February 1, 2015

As evidenced within our review of the various use cases, AirWatch controls consistently meet or exceed those within the existing Microsoft ActiveSync system. However, the AirWatch controls as currently configured are generally minimal, as compared to the new product’s functionality and capabilities, and mimic the limited controls within the existing Microsoft ActiveSync system. Subsequent product maturation and enhancements should be appropriately based upon documented risk management decisions after performing a formal risk assessment. Pursuant to related practice standards, planned enhancements and product maturation will require UTMB Health’s Institutional Security and Privacy Compliance Committee approval.

Recommendation 2014-027-03-R:
Information Services Operations, working with the Office of Information Security, should conduct a risk assessment of the mobile computing and communications environment. This assessment process should determine UTMB Health’s risk position and provide the basis for evaluation of subsequent enhancements of AirWatch controls and modifications to related practice standards.

Management’s Response: The Office of Information Security, working with Information Services, will conduct a risk assessment of the mobile computing and communications environment.

Implementation Date: July 1, 2015

Lessons Learned
To continuously improve processes and increase IT investment success rates, any implementation review should include a summary of major lessons learned. A careful review of these successes and improvement opportunities allows the institution to benefit from innovations, enhancements, corrections, or hindrances occurring during the project. Additionally, the review can provide valuable information for decreasing costs and risks in future projects. Lessons learned specifically identified during this pilot project review include:

Areas of Success or Project Strengths:
• Controls and capabilities of new MDM solution (AirWatch) meet or exceed that of existing system (Microsoft ActiveSync)
• Pilot use cases have been relatively seamless as implemented, while generally transparent to most end users, Patient Services cited significant improvement in controls

Areas of Opportunity or Improvement:
• Establish a clear sense of ownership for institutional implementation with greater collaboration between IS Operations and the Office of Information Security
Mobile Device Management Solution Implementation Review
Engagement Number 2014-027

- Consistent adherence to standardized project management process/practices

As the IT Governance process continues to mature, the MyUTMB project/service request tracking system will soon be replaced with a scalable project management solution to help address the identified opportunities. This replacement project is presently in final scoping.

Additional Information
As an added measure to ensure the development of reasonable and prudent controls, organizations should periodically benchmark against peers and evaluate industry codes of best practice.

When compared to peers:
- No UT System institution has yet reported completion of an enterprise implementation of AirWatch
- Initial controls as planned and approved for UTMB Health’s enterprise implementation of AirWatch are comparable to controls as required by peers
- When cited specifically, Epic Haiku (smartphone) and Canto (iPad) applications require enrollment in AirWatch to ensure secure access to authorized clinical users of Epic’s electronic health record (UTMB Health requirement pending enterprise implementation)
- Deletion of ActiveSync prior to AirWatch enrollment/registration process to avoid creation of duplicate accounts

When compared to industry codes of best practice, such as Control Objectives for Information and Related Technology (COBIT), The United States Department of Health and Human Services (HHS), and AirWatch, pertinent guidance includes the following:
- Know the business value and risk of mobile device use, the mobile device environment should be formally defined to determine what should and shouldn’t be included, particularly for personally owned devices
- Establish security governance over mobile devices, strategy and controls should be based upon formally documented risk management decisions (e.g., AirWatch registration/enrollment for mobile devices not identified through ActiveSync)

Conclusion
In preparation for an institutional enterprise-wide implementation, UTMB Health has implemented a small number of use cases as an evaluation and testing pilot of the new Mobile Device Management solution (AirWatch). As outlined in the request for proposal and scope of work, the pilot project achieved stated business goals and objectives; however, the standardized project management process was not consistently followed. Areas of opportunity for improvement include creating scalability within the standardized project management process for those projects not involving substantial enterprise systems and project tracking for phased implementations, revision of applicable practice standards to reflect the current or desired state of operations, and a
formal determination of related risk to serve as the basis for evaluating future enhancements to product controls and corresponding practice standards.

We greatly appreciate the assistance provided by staff from the Office of Information Security, Office of Institutional Compliance, Nursing Services Administration, Patient Services, Surgery, Information Services, and from the Office of The University of Texas Systemwide Information Security Compliance and hope that the information presented in our report is beneficial.

Kimberly K. Hagara, CPA, CIA, CISA, CRMA
Associate Vice President, Audit Services

Randal J. Crawford, CISSP, CIA, CISA, CRISC, CGEIT
IT Audit Services Manager