UNIVERSITY OF VIRGINIA
BOARD OF VISITORS
MEETING OF THE
AUDIT AND COMPLIANCE COMMITTEE
FEBRUARY 26, 2010
AUDIT AND COMPLIANCE COMMITTEE
(Open Session)

Friday, February 26, 2010
8:30 - 9:00 a.m.
Board Room, The Rotunda

Committee Members:
W. Heywood Fralin, Chair
Helen E. Dragas                   Don R. Pippin
Austin Ligon                    Warren M. Thompson
Vincent J. Mastracco, Jr.       John O. Wynne, Ex-officio

AGENDA

<table>
<thead>
<tr>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. INFORMATION REPORT (Ms. Deily)</td>
</tr>
<tr>
<td>A. Auditor of Public Accounts (APA) Audit and Management Letter (Ms. Deily to introduce Mr. Walter Kucharski, Auditor of Public Accounts of the Commonwealth; Mr. Kucharski to report)</td>
</tr>
<tr>
<td>B. Audit Department Status Report for Fiscal Year 2009 - 2010</td>
</tr>
<tr>
<td>C. Summary of Audit Findings (Ms. Deily)</td>
</tr>
<tr>
<td>D. HIPAA Privacy Status (Written Report)</td>
</tr>
</tbody>
</table>

II. EXECUTIVE SESSION - LIST OF ITEMS

III. APPROVAL OF SUMMARY OF AUDIT FINDINGS (resolution) 15
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: February 26, 2010

COMMITTEE: Audit and Compliance

AGENDA ITEM: I.A. Auditor of Public Accounts

ACTION REQUIRED: None

BACKGROUND: The Auditor of Public Accounts of the Commonwealth conducts an annual audit of the University and the Medical Center and reports to the Board on his findings. Ms. Deily will introduce the Auditor, Mr. Walter Kucharski, who will report. University management will respond to the Auditor’s Audit and Management letter.
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: February 26, 2010

COMMITTEE: Audit and Compliance

AGENDA ITEM: I.B. Audit Department Status Report, 2009 – 2010

ACTION REQUIRED: None

BACKGROUND: Ms. Deily will inform the Board of the status of audit projects of the Audit Department for the current Fiscal Year. This report does not require formal action, but is information of which the Board should be made aware.
### Scheduled Audit Projects

<table>
<thead>
<tr>
<th></th>
<th>University</th>
<th>Health System</th>
<th>IT</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled</td>
<td>12</td>
<td>13</td>
<td>5</td>
<td>30</td>
</tr>
<tr>
<td>Completed</td>
<td>5</td>
<td>6</td>
<td>2</td>
<td>13</td>
</tr>
<tr>
<td>% Completed</td>
<td>42%</td>
<td>46%</td>
<td>40%</td>
<td>43%</td>
</tr>
<tr>
<td>In Process</td>
<td>5</td>
<td>5</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>% In Process</td>
<td>42%</td>
<td>38%</td>
<td>20%</td>
<td>37%</td>
</tr>
<tr>
<td>% Complete or In Process</td>
<td>83%</td>
<td>85%</td>
<td>60%</td>
<td>80%</td>
</tr>
</tbody>
</table>

### Non-Scheduled Projects

<table>
<thead>
<tr>
<th></th>
<th>University</th>
<th>Health System</th>
<th>IT</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carry-forward</td>
<td>11</td>
<td>4</td>
<td>0</td>
<td>15</td>
</tr>
<tr>
<td>New</td>
<td>9</td>
<td>9</td>
<td>11</td>
<td>29</td>
</tr>
<tr>
<td>Total</td>
<td>20</td>
<td>13</td>
<td>11</td>
<td>44</td>
</tr>
<tr>
<td>Completed</td>
<td>16</td>
<td>8</td>
<td>10</td>
<td>34</td>
</tr>
<tr>
<td>% Completed</td>
<td>80%</td>
<td>62%</td>
<td>91%</td>
<td>77%</td>
</tr>
<tr>
<td>In Process</td>
<td>4</td>
<td>5</td>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>% In Process</td>
<td>20%</td>
<td>38%</td>
<td>9%</td>
<td>23%</td>
</tr>
<tr>
<td>% Complete or In Process</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: February 26, 2010

COMMITTEE: Audit and Compliance

AGENDA ITEM: I.C. Summary of Audit Findings

ACTION REQUIRED: None

BACKGROUND: Ms. Deily will present a summary of audit findings on the following audit reports: Department of Medicine Enterprise Reporting System, School of Medicine Follow-Up, John Paul Jones Arena, and Delegation of Authority.
AUDIT DEPARTMENT
EXECUTIVE SUMMARY

Department of Medicine Enterprise Reporting System  October 26, 2009

BACKGROUND

The Enterprise Reporting System was developed by the Department of Medicine as a tool to improve financial reporting and expand access to financial data by departmental employees and members of the faculty. Several departments in the School of Medicine (Medicine, Radiology, and Pediatrics) rely on the system to provide reports on clinical billing, financial performance, faculty remuneration and research administration.

AUDIT OBJECTIVES

The objectives of the audit were to (1) determine whether system access and security were reasonable and in compliance with applicable computing policies and safe computing procedures; (2) evaluate the controls over the acquisition and maintenance of enterprise data; and (3) determine the level of use and satisfaction with the system.

OPINION ON AUDIT OBJECTIVES

Overall, we found the system to be a useful tool in the area of financial and management reporting. The controls over the acquisition and maintenance of enterprise data were adequate to ensure that reliable reports were provided to users of the system. Initially, access to the system was not sufficiently secured in that users were provided default passwords that could be used by others to gain unauthorized access to the system. However, this condition was corrected during the course of the audit. In addition, opportunities were identified to improve awareness of the system and to increase the level of use among faculty members.

AREA NOTED FOR IMPROVEMENT

1) Opportunities existed to increase the use of the system through outreach and educational efforts within the department.

MANAGEMENT’S RESPONSE

Management concurs and has agreed to correct the identified condition.

FINANCIAL IMPACT

Changes to system security have helped prevent unauthorized access to confidential data. Improved education about the system should provide opportunities for enhanced performance through more widely-used management reporting tools.
BACKGROUND

The Audit Department has completed a follow-up audit of the implementation of suggested actions noted in the School of Medicine (SOM) audit reports and memoranda for which SOM management responded that corrective action had been taken between July 1, 2008, and June 30, 2009. During the follow-up audit, the Audit Department completed a risk analysis of the seven previously identified issues included in three audit reports and memoranda. Based upon the results of the analysis, six issues were deemed to be continuously monitored on a School-wide level via the Audit Department’s compliance audits, and the annual ARMICS review or regularly scheduled Fiscal Year 2010 audits. Therefore, follow-up testing during this audit was conducted on the remaining outstanding issue.

AUDIT OBJECTIVES

The primary objectives of a follow-up audit are to ensure that the suggested actions are addressed on a timely basis and that the corrective action satisfactorily resolves the initial business issues communicated to management.

OPINION ON AUDIT OBJECTIVES

Based on follow-up testing results, the outstanding issue has been satisfactorily addressed. Specifically, the SOM revised one policy and implemented a new policy covering clinical trial billing and budgeting practices.

FINANCIAL IMPACT

Suggested actions made by the Audit Department help to improve controls over the School of Medicine’s operations.
BACKGROUND

The John Paul Jones Arena (the Arena) is home to the University of Virginia’s Men’s and Women’s Basketball teams and host to a myriad of attractions including concerts, family shows, and community events. The Arena opened in August 2006, and is the largest arena in the Commonwealth of Virginia. Pursuant to a contract dated May 9, 2005, SMG has agreed to act as the exclusive manager of the Arena. As part of this role, SMG has agreed that the Arena’s daily operations will be subject to the University’s policies and the decisions of the University’s Contract Administrator.

AUDIT OBJECTIVE

The objective of the audit was to review the University’s administrative oversight process for disbursing complimentary tickets for events held at the Arena. Originally, the intended scope of the audit was to assess the level of compliance between the Arena’s daily operations and the May 2005 contract between the University and SMG. During the planning phase of the audit, however, Audit learned that an independent CPA firm had already conducted agreed-upon procedure engagements of the Arena for the past two years. Audit reviewed the list of agreed-upon procedures performed by the independent CPA firm for the fiscal year ended June 30, 2008, and deemed the procedures to be reasonable and adequate.

OPINION ON AUDIT OBJECTIVE

Our opinion, based on the fieldwork we completed in support of the stated audit objective, is that internal controls need to be strengthened to improve the University’s administrative oversight of complimentary tickets disbursed for events held at the Arena.

AREA NOTED FOR IMPROVEMENT

Currently, the University’s Office of Business Operations does not have a written policy in place that defines how complimentary tickets for events at the Arena are or should be disbursed in accordance with applicable University policies.

MANAGEMENT’S RESPONSE

Management concurs and has agreed to correct the identified condition.
FINANCIAL IMPACT

Implementation of the suggested action will enhance internal controls and improve compliance with regulatory policies.
BACKGROUND

The execution of contracts is a means of procuring the goods and services necessary to support the purpose and goals of the University. All contracts must be made in accordance with the laws of the Commonwealth and comply with established policies and procedures of the University. Distinct series of financial and administrative policies govern the two basic types of contracts at the University: those associated with sponsored programs, and those not related to sponsored programs. This audit focused on those contracts not related to sponsored programs. These contracts must be signed for the Rector and Visitors of the University of Virginia by an authorized signatory. Authorized signatories by the Board of Visitors include the President, the Executive Vice President and Chief Operating Officer, and the Vice President and Chief Financial Officer. To expedite the review and processing of contracts, limited authority to sign certain agreements has been further delegated in writing to designated administrative officers.

AUDIT OBJECTIVES

The objectives of the review were to determine whether, for contracts not related to sponsored programs:

- people signing contracts had the authority to do so; and
- contracts signed via delegation of authority were: a) within the scope of authority delegated, and b) did not include specific inappropriate terms.

OPINION ON AUDIT OBJECTIVES

Based upon the test work performed, the contracts signed via delegation of authority were in compliance with State and University policies. Specifically, the contracts we reviewed were within the scope of the signatories’ authority, and no instances of inappropriate terms being included in the contracts were noted during the audit. Although we did not become aware of any individuals signing contracts who did not have the authority to do so, we recognize that these situations might exist at the institution. Contracts associated with the following departments were tested: Athletics, Business Operations, University Library, Darden, Facilities Management, Housing Division, L.P. Jackson Cultural Center, and Procurement Services.
FINANCIAL IMPACT

Noncompliance with the University’s signatory authority policy could result in the University being committed to inappropriate contracts.
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: February 26, 2010

COMMITTEE: Audit and Compliance

AGENDA ITEM: I.D. HIPAA Privacy Status Report

ACTION REQUIRED: None

BACKGROUND: The Economic Stimulus law made significant changes in the HIPAA Privacy and Security Rules. These changes will:

1) extend the reach of the HIPAA Privacy and Security Rules,
2) impose privacy breach notification requirements,
3) increase enforcement of the Privacy and Security Rules, and
4) impose harsher penalties for violations of privacy and security.

Implications for the University of Virginia:

Many of the changes are being phased in over time. Importantly, the changes make clear that any individual can be convicted of criminal violations if he/she intentionally and wrongfully acquires or discloses patient information. The new penalties for violations of privacy and security of patient information became effective when the Economic Stimulus law was signed in February 2009. Enforcement of the other new provisions is being phased in, with many becoming effective in February 2010.

We have educated our employees on the changes and their potential criminal liability through presentations at Manager’s and Staff meetings and inclusion of this material in our mandatory training modules completed upon hire and annually. Medical Center policies and procedures have been updated to include relevant material. Ongoing education via these methods will continue as changes in the HIPAA Privacy and Security Rules become effective.

The Compliance and Privacy Office conducts routine audits to monitor for violations of privacy and security of patient information. All employees have an obligation to report suspected misconduct including any violation of policies and procedures and patient confidentiality. The Compliance and Privacy Office conducts a risk assessment on all observed or reported violations, to determine if privacy breach notification is required.
The breach notification requirements generally apply to any use or disclosure of patient information that is impermissible under the Privacy Rule and that compromises the security or privacy of the information such that the use or disclosure poses a significant risk of financial, reputational, or other harm. Patients must be notified in writing of any breaches. Also, we are required to report all breaches to the Department of Health and Human Services. For breaches that involve fewer than 500 patients, we report on an annual basis. For those that involve 500 or more individuals, media notification and immediate notice to the Secretary may be required. Breach notification became effective September 23, 2009, with our first report due within 60 days from the end of the 2009 calendar year. We have three breaches to report for 2009. This report does not require formal action, but is information of which the Board should be made aware.