UNIVERSITY OF VIRGINIA
BOARD OF VISITORS
MEETING OF THE
AUDIT AND COMPLIANCE
COMMITTEE
MARCH 24, 2015
AUDIT AND COMPLIANCE COMMITTEE
(Open Session)

Tuesday, March 24, 2015
10:30 – 11:30 a.m.
Byrd Room, Harrison Institute

Committee Members:
Frank E. Genovese, Chair
L.D. Britt, M.D.
Allison Cryor DiNardo
Barbara J. Fried
William H. Goodwin Jr.
George Keith Martin, Ex-officio
Adelaide Wilcox King, Faculty Consulting Member

AGENDA

I. INFORMATION REPORTS (Mr. Gary S. Nimax)
   A. Corporate Compliance and Privacy Office
      Status Report for Fiscal Year 2014 – 2015
      (Mr. Nimax to introduce Ms. Lori J. Strauss;
       Ms. Strauss to report)
   B. Report on Enterprise Risk Management
   C. Audit Department Status Report for Fiscal Year 2014 – 2015
   D. Summary of Audit Findings

II. EXECUTIVE SESSION – LIST OF ITEMS

III. ACTION ITEM
    • Approval of the Compliance and Privacy Office
      Findings and the Summary of Internal Audit Department Findings
BOARD MEETING: March 24, 2015

COMMITTEE: Audit and Compliance

AGENDA ITEM: I.A. Corporate Compliance and Privacy Office
Status Report for Fiscal Year 2014 – 2015

ACTION REQUIRED: None

BACKGROUND: Ms. Strauss will inform the Board of the status of compliance projects of the Corporate Compliance and Privacy Office for the current fiscal year. This report does not require formal action, but is information of which the Board should be made aware.
## Corporate Compliance & Privacy Office
### Scheduled Projects 2014-15

<table>
<thead>
<tr>
<th>Projects</th>
<th>Scheduled Hours</th>
<th>Revised Scheduled Hours</th>
<th>Projects In Process (%)</th>
<th>Projects Completed (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outpatient Department Coding, Billing &amp; Documentation</td>
<td>800</td>
<td>250</td>
<td>1 (100%)</td>
<td>0 (0%)</td>
</tr>
<tr>
<td>Privacy Monitoring &amp; Auditing: Monthly Site Visits</td>
<td>400</td>
<td>400</td>
<td>3 (8%)</td>
<td>18 (50%)</td>
</tr>
<tr>
<td>Inpatient Medicare Severity Diagnosis Related Groups:</td>
<td>1,200</td>
<td>530</td>
<td>1 (33%)</td>
<td>2 (67%)</td>
</tr>
<tr>
<td>Correct Coding &amp; Medical Necessity</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance &amp; Privacy Training: Annual, New Hire, Hybrid</td>
<td>400</td>
<td>400</td>
<td>2 (20%)</td>
<td>2 (20%)</td>
</tr>
<tr>
<td>Total</td>
<td>2,800</td>
<td>1,580</td>
<td>7 (15%)</td>
<td>22 (46%)</td>
</tr>
</tbody>
</table>

With the revised project schedule that was presented at the November Audit & Compliance Committee meeting, there are 48 scheduled projects with 22 (46%) of these projects complete and seven (15%) projects in process. The Office had a staff analyst vacancy one month into the fiscal year that resulted in the need to revise the Office's project schedule. The Office rehired an experienced analyst who began employment in January 2015. The Office is on target to have all scheduled projects completed by the end of the fiscal year.
OTHER PROJECTS

Training: The Office updated the compliance and privacy content for the mandatory retraining module. The revised content provided education on trends that were identified during site visits, changes to compliance or privacy related policies and procedures, questions from staff or management, and the Office’s auditing and monitoring program. Training was included on such things as the need to log off of computers when unattended; the need to double-check papers containing protected health information (PHI) before providing the papers to patients; the Medical Center’s policies and procedures regarding access to the medical record and the use and storage of PHI on mobile devices, such as laptop computers, mobile phones and flash drives; clarification of what MyChart is; the need to use proper safeguards when transporting documents; and clarification of the conflict of interest policy.

The Office provided seven department-specific privacy presentations for six areas (School of Nursing, Patient Relations, Language Services, Crossroads Family Practice, Infectious Disease Clinic, and Hematology/Oncology Clinic).

The 14 hybrid departments that were identified as part of the Medical Center’s covered entity, and in turn needing to be trained on the Health Insurance Portability and Accountability Act (HIPAA), were contacted resulting in the Office assigning and ensuring completion of the new hire privacy and electronic security training module for 68 employees.

Consulting: The Office is consulted regularly by staff, management, clinicians, and others to locate regulations, provide input to Medical Center policy and procedure revisions related to compliance and privacy practices, clarify policies and procedures related to such things as gifts or accessing medical records, conduct privacy audits and site reviews to ensure physical safeguards are sufficient to protect health information, and provide guidance on such things as the type of information that can be placed on electronic boards in patient care areas.

The Office is represented on several committees to provide guidance on compliance and privacy related issues. Some of these committees are the Grievance, Joint Commission Steering, Quality, Health Information Management, Medical Center Management, Operations Leadership, and Payer Audit Review committees.
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: March 24, 2015

COMMITTEE: Audit and Compliance

AGENDA ITEM: I.B. Report on Enterprise Risk Management (ERM)

ACTION REQUIRED: None

BACKGROUND: At its June 2014 meeting, Gary Nimax, who is the Assistant Vice President for Compliance and Enterprise Risk Management and also the Interim Chief Audit Executive, reviewed the University’s ERM program with the Board. The Board discussed nine institutional risk categories, along with more specific subcategories, that represent the key institutional risks for the academic division. The University’s vice presidents and deans provided feedback in developing and ranking these risks and board members were encouraged to provide feedback.

As the Assistant Vice President for Compliance and Enterprise Risk Management, Mr. Nimax’s responsibilities include the direction of a compliance and enterprise risk management program, as well as the supervision of the Director of Property and Liability Risk Management and the Medical Center’s Chief Corporate Compliance and Privacy Officer.

Mr. Nimax has worked at the University since 1989 in a variety of administrative roles, including positions as a buyer in the medical center, as Assistant Director of Procurement Services for the Academic Division, as team lead for the Integrated Systems Project, as Assistant to the Vice President for Management and Budget, and most recently as the Assistant Vice President and Director of University-Related Foundation Administration.

Mr. Nimax earned his undergraduate degree from U.Va. and his Master of Business Administration from James Madison University. He obtained his professional certification as a Certified Compliance and Ethics Professional (CCEP) through the Society of Corporate Compliance and Ethics.
DISCUSSION: Mr. Nimax will review the documentation developed to outline the mitigation strategies identified to manage key institutional risks. The University will complete a similar summary for each risk, beginning with the risks associated with the management of human capital.
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: March 24, 2015

COMMITTEE: Audit and Compliance

AGENDA ITEM: I.C. Audit Department Status Report for Fiscal Year 2014 – 2015

ACTION REQUIRED: None

BACKGROUND: Mr. Gary Nimax will inform the Board of the status of Audit Department projects for the current fiscal year. This report does not require formal action, but is information of which the Board should be made aware.
UNIVERSITY OF VIRGINIA
AUDIT DEPARTMENT

Status of Fiscal Year 2014-15 Audit Projects
as of December 31, 2014

Scheduled Audit Projects

<table>
<thead>
<tr>
<th></th>
<th>University</th>
<th>Hospital &amp; IT</th>
<th>Internal Control Compliance</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scheduled</strong></td>
<td>11*</td>
<td>13</td>
<td>4</td>
<td>28</td>
</tr>
<tr>
<td><strong>Completed</strong></td>
<td>4</td>
<td>2</td>
<td>2</td>
<td>8</td>
</tr>
<tr>
<td><strong>% Completed</strong></td>
<td>46%</td>
<td>15%</td>
<td>50%</td>
<td>29%</td>
</tr>
<tr>
<td><strong>In Process</strong></td>
<td>3</td>
<td>9</td>
<td>1</td>
<td>13</td>
</tr>
<tr>
<td><strong>% In Process</strong></td>
<td>27%</td>
<td>70%</td>
<td>25%</td>
<td>46%</td>
</tr>
<tr>
<td><strong>% Complete or In Process</strong></td>
<td>73%</td>
<td>85%</td>
<td>75%</td>
<td>75%</td>
</tr>
</tbody>
</table>

* One audit was deleted due to grant contract terms requiring an external review.

Non-Scheduled Projects

<table>
<thead>
<tr>
<th></th>
<th>University</th>
<th>Hospital &amp; IT</th>
<th>Internal Control Compliance</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Carry-forward</strong></td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td><strong>New</strong></td>
<td>4</td>
<td>6</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>8</td>
<td>6</td>
<td>0</td>
<td>14</td>
</tr>
<tr>
<td><strong>Completed</strong></td>
<td>5</td>
<td>5</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td><strong>% Completed</strong></td>
<td>63%</td>
<td>83%</td>
<td>0%</td>
<td>71%</td>
</tr>
<tr>
<td><strong>In Process</strong></td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td><strong>% In Process</strong></td>
<td>37%</td>
<td>17%</td>
<td>0%</td>
<td>29%</td>
</tr>
<tr>
<td><strong>% Complete or In Process</strong></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: March 24, 2015

COMMITTEE: Audit and Compliance

AGENDA ITEM: I.D. Summary of Audit Findings

ACTION REQUIRED: None

BACKGROUND: Mr. Nimax will present a summary of audit findings on the following audit report: FY 2014 IT Audit Follow-Up Review.
BACKGROUND

The Audit Department has completed a follow-up audit of significant information technology audit issues with remediation due dates in the fiscal year 2014. Significant issues were those issues summarized in each audit report’s executive summary. The Audit Department uses a three-year information technology (IT) audit plan to audit all areas required by the International Organization for Standards (ISO) 27002 related to information security. ISO 27002 also is applied to the University’s IT management and security practices. At the end of each audit with reportable issues, management responded that corrective action would be taken by certain dates. As required by the Institute of Internal Auditors’ Standard 2500, follow-up audit work is an important step to ensure accountability and that remedial actions have occurred, are receiving adequate management attention, or management has accepted the risk of not taking action.

AUDIT OBJECTIVE

The objective of a follow-up audit is to ensure that the initial areas noted for improvement as communicated to management are resolved in a timely and satisfactory manner.

OPINION ON AUDIT OBJECTIVE

Overall, University management had satisfactorily addressed the majority of issues identified in the original audits. In total there were twenty-one significant issues identified among all audits with completion due dates within fiscal year 2014, and all but one had been satisfactorily addressed by management.

AREA NOTED FOR IMPROVEMENT

The University had an outstanding issue related to proper update of phone directory records. Delay of the Identity Management System Project due to resource constraints prevented remediation of this issue. In the interim, while awaiting continuation of the project, on-going prompts to users to review and update phone directory information were encouraged.

MANAGEMENT’S RESPONSE

Management concurs and has agreed to address the outstanding issue.
BOARD MEETING: March 24, 2015

COMMITTEE: Audit and Compliance

AGENDA ITEM: III. Approval of Corporate Compliance and Privacy Office Findings and the Summary of Internal Audit Findings

BACKGROUND: This resolution reflects discussion by the Committee, in Executive Session, of a summary of recent projects conducted by the Corporate and Privacy Compliance Office and a summary of recent internal audit findings.

ACTION REQUIRED: Approval by the Audit and Compliance Committee and by the Board of Visitors

SUMMARY OF COMPLIANCE AND PRIVACY FINDINGS AND SUMMARY OF INTERNAL AUDIT FINDINGS

RESOLVED, the Summary of Compliance Projects for the period July 1, 2014 through December 31, 2014, as presented by the Chief Corporate Compliance and Privacy Officer, and the Summary of Internal Audit Findings for the period October 16, 2014 through December 31, 2014, as presented by the Interim Chief Audit Executive, are approved.