UNIVERSITY OF VIRGINIA
BOARD OF VISITORS
MEETING OF THE
AUDIT, COMPLIANCE, AND
RISK COMMITTEE
SEPTEMBER 16, 2016
AUDIT, COMPLIANCE, AND RISK COMMITTEE
(Open Session)

Friday, September 16, 2016
1:00 – 2:00 p.m.
Board Room, The Rotunda

Committee Members:
Frank E. Genovese, Chair
Mark T. Bowles
L. D. Britt, M.D.
Frank M. Conner III
Babur B. Lateef, M.D.
James B. Murray Jr.
William H. Goodwin Jr., Ex-officio
Adelaide Wilcox King, Faculty Consulting Member

AGENDA

I. REMARKS BY THE COMMITTEE CHAIR (Mr. Genovese) 1

II. REPORT
   • UVA Medical Center’s Corporate Compliance & Privacy  2
     Office Summary of Fiscal Year 2016 (Written Report)

III. DISCUSSION
   A. Audit Department Activities (Mr. Genovese to introduce  5
      Ms. Carolyn D. Saint; Ms. Saint to report)
      • Audit Plan Status and Department Current Activities  6
   B. University Compliance (Mr. Genovese to introduce  11
      Mr. Gary S. Nimax; Mr. Nimax to report)
      • Report on Medical Center Compliance and Privacy  11
        Officer Search
   C. Enterprise Risk Management (ERM) Report (Mr.  12
      Genovese to introduce Mr. James S. Matteo and Mr.
      Michael R. Marquardt; Messrs. Matteo and Marquardt to
      report)

IV. CLOSED SESSION
   • Discussion of Medical Center operations as provided  12
      for in Section 2.2-3711(A)(22) of the Code of Virginia.
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: September 16, 2016

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: I. Remarks by the Committee Chair

ACTION REQUIRED: None

BACKGROUND: Mr. Frank Genovese, the Committee Chair, will open the meeting and provide an overview of the agenda.
II. Report: UVA Medical Center’s Corporate Compliance & Privacy Office Summary of Fiscal Year 2016

Scheduled Projects

The Fiscal Year 2016 Corporate Compliance & Privacy ("Office") project schedule contemplated scheduled projects in these areas: audits related to reimbursement for inpatient, outpatient, or procedural services; privacy auditing and monitoring; and, developing and conducting training.

Inpatient, Outpatient and Procedure Area Audits

The Office completed seven out of the eight projects scheduled. The one project was not completed due in part to a staff vacancy that occurred in April 2016, but it will be completed in Fiscal Year 2017.

Five billing, coding, and documentation projects not previously reported were additionally conducted in Fiscal Year 2016: 1) exclusion audit; 2) inpatient medical severity-diagnosis related group (MS-DRG) correct coding and medical necessity for intracranial hemorrhage; 3) inhalation treatments; 4) Intensity Modulated Radiotherapy Treatment (IMRT) Plan; and 5) Managed Care Organization (MCO) payments for services after beneficiaries’ death. No significant findings were identified in these projects.

Privacy Auditing & Monitoring

The office conducted 36 privacy site audits (10 inpatient units, 11 procedure areas, and 15 outpatient clinics). At least three locations are visited each month. The office coordinates visits with management and provides a written summary of the findings. Random electronic medical record access audits of patients seen in the sites visited were performed. One-hundred and eighty (180) medical record access reviews were done finding no unauthorized accesses.

Recommendations and education during the site audits address physical, administrative, and technical safeguards for protected
Developing and Conducting Training

The Office revised, and provided the annual training and new hire modules on compliance, privacy, electronic-protected health information (e-PHI) security, and ethics. The Office prepared monthly privacy reminders for the Medical Center’s Management Group highlighting topics from the Department of Health and Human Services Office for Civil Rights, audit trends, and policy changes that are shared with employees.

Unscheduled Projects

The Office allows time in the project schedule for unknown projects and investigations due to changes in regulation; the need for consultation and department specific training; policy and procedure review and guidance; and, compliance and HIPAA privacy investigations that are not known at the beginning of the Fiscal Year, but that arise during the Fiscal Year.

Consulting; Developing and Conducting Training

The Office was sought for compliance and privacy guidance by the Medical Center’s Security staff related to data loss prevention reports involving PHI, and ransomware incidents, Continuum Home Health for compliance with billing regulations, the Emergency Department for guidance on inclusion in a statewide Emergency Medical Services database, and the School of Medicine for privacy-related guidance. Guidance was offered on compliance and privacy issues for several committees. The Office reviewed and provided feedback on multiple Medical Center policies and procedures. Guidance was provided to members of management and staff on such topics as medical record accesses, use of MyChart, and interactions with law enforcement.

Six department-focused privacy and compliance presentations were done for the departments of Ophthalmology, Neuro-Radiology, Pharmacy, and Graduate Medical Education (three presentations).

Compliance and HIPAA Privacy

The Office encourages employees to report any perceived violation. The Office has a robust reporting system, which includes an anonymous Help Line, and a commitment to employees that the Office has an open line of communication for employees to report in good faith any perceived violation and/or suspected misconduct.
without being subject to retaliation. As evidenced by the number of investigations, our employees have been educated and are encouraged to report concerns and they know where to report. Our investigations involve working with the Medical Center, School of Medicine, School of Nursing, and University Physicians Group to ensure that the policies and sanctions are consistent for violations of confidentiality.

Requests were received by the Office in Fiscal Year 2016 to review 685 unanticipated compliance or HIPAA privacy related projects, inquiries, or investigations this fiscal year. This included preparing and analyzing audit reports of electronic medical records, providing guidance to management and staff on policy interpretation, and investigating compliance and privacy issues as reported by patients, family members, or visitors to the Medical Center.

Compliance

The Office investigated 112 compliance issues in Fiscal Year 2016 with seven of these issues being reported through the Compliance Helpline. No significant compliance issues were identified for the Medical Center from these reviews.

HIPAA Privacy

The Office conducted 573 privacy investigations during Fiscal Year 2016 resulting in sanctions for 118 individuals. The number of privacy investigations increased in Fiscal Year 2016 (573) compared to Fiscal Year 2015 (520). The trend for the last three years has been an increase in the number of paper related investigations, and remains a focus of the Office.
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: September 16, 2016

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: III.A. Audit Department Activities

ACTION REQUIRED: None

BACKGROUND: For purposes of supporting the Committee’s oversight of the Audit Department, Ms. Carolyn Devine Saint, Chief Audit Executive, will summarize the Audit Department’s activities for FY 2017 year to date.
## Report to BOV ACR Committee:
**September 2016 Audit Department Status**

### Assurance and Advisory Projects: Completed FY 2017 To Date

<table>
<thead>
<tr>
<th>Subject</th>
<th>UVA Division</th>
</tr>
</thead>
<tbody>
<tr>
<td>Curry School of Education</td>
<td>Academic</td>
</tr>
<tr>
<td>Darden Fund Transfers</td>
<td>Academic</td>
</tr>
<tr>
<td>Distributed IT Systems Current State Assessment</td>
<td>Academic</td>
</tr>
<tr>
<td>FY2016 Inventories (UVA Bookstore, Pharmacy)</td>
<td>Academic, Health System</td>
</tr>
<tr>
<td>Action Plan Implementation Status—Follow Ups</td>
<td>Academic, Health System</td>
</tr>
</tbody>
</table>

### Assurance and Advisory Projects: In Progress as of September 2016 BOV Meeting

<table>
<thead>
<tr>
<th>Subject</th>
<th>UVA Division</th>
</tr>
</thead>
<tbody>
<tr>
<td>Epic(^1) Phase 2 Implementation—Project Health Check w/ IT Security Focus</td>
<td>Health System</td>
</tr>
<tr>
<td>Fiscal Stewardship (Data-driven Internal Controls Analytics) Proof of Concept</td>
<td>Academic</td>
</tr>
<tr>
<td>Integrated Assurance – Compliance Assessment</td>
<td>Academic</td>
</tr>
<tr>
<td>System Security: Privileged Access (Core Systems)</td>
<td>Health System</td>
</tr>
<tr>
<td>Ivy Cloud (^2) — Project Health Check w/ Security and Governance Focus</td>
<td>Pan-University</td>
</tr>
<tr>
<td>Security Enhancement Plan (SEP) Project Health Check</td>
<td>Academic</td>
</tr>
<tr>
<td>SCADA(^3) Consultation</td>
<td>Pan University</td>
</tr>
</tbody>
</table>

### Current View of Risk Prioritized Future Projects (Remainder of FY17)

<table>
<thead>
<tr>
<th>Subject</th>
<th>UVA Division</th>
</tr>
</thead>
<tbody>
<tr>
<td>340B Drug Discount Program</td>
<td>Health System</td>
</tr>
<tr>
<td>Environmental Health &amp; Safety Compliance</td>
<td>Health System</td>
</tr>
<tr>
<td>HIPAA Risk Assessment</td>
<td>Academic</td>
</tr>
<tr>
<td>Uniform Guidance Implementation: Consultation with Office of Sponsored Programs</td>
<td>Academic</td>
</tr>
<tr>
<td>ARMICS (Agency Risk Management and Internal Control Standards) Consultation</td>
<td>Academic</td>
</tr>
<tr>
<td>Epic Phase 2 Implementation—Project Health Check w/ Control Framework Focus</td>
<td>Health System</td>
</tr>
<tr>
<td>Strategic Investment Fund Expenditures Monitoring</td>
<td>Pan-University</td>
</tr>
<tr>
<td>UFirst HR Transformation—Project Health Check</td>
<td>Pan-University</td>
</tr>
<tr>
<td>IT Change Controls</td>
<td>Health System</td>
</tr>
<tr>
<td>Presidential Travel and Expenses</td>
<td>Pan-University</td>
</tr>
</tbody>
</table>

---

\(^1\) Epic is UVA Health System’s Electronic Medical Records system. Phase 2 implements Epic’s scheduling and revenue cycle modules.

\(^2\) UVA Data Science Institute’s cloud computing environment for highly sensitive, secure data for researchers

\(^3\) SCADA=Supervisory Control and Data Access. SCADA is a system for remote monitoring and control that operates with coded signals over communication channels.
The chart below illustrates the Audit Department’s assurance and advisory projects by UVA division (Academic, Health System, and Pan University). This is a proxy for risk coverage and shows at a glance the increasing activity in the Health System from prior years.

The chart below summarizes the various types of work we perform, demonstrating the increasing relevance of the Audit Department to in-flight projects. In addition to the core assurance projects we undertake, the Audit Department is more frequently involved at the beginning of higher risk and strategically important projects—staying with them as the work rolls out. We provide consulting on risks and controls, and perform Project Health Checks that provide an objective perspective to project leaders and sponsor on risks to successful implementation.
The Audit Department monitors the status of management’s action plans to remediate control deficiencies, communicated in our reports, as their planned implementation dates approach. The tables below summarize current status of action plans with due dates from July 1, 2015 through August 31, 2016. Refer to the Appendix that follows for detail on open Priority 1 action plans.

**Action Plan Completion Status by Priority Rating**

<table>
<thead>
<tr>
<th>Priority 1</th>
<th>Priority 2</th>
<th>Legacy (Unrated)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>25</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

**Action Plan Completion Status by UVA Division**

<table>
<thead>
<tr>
<th>UVA Division</th>
<th>Closed</th>
<th>Open</th>
</tr>
</thead>
<tbody>
<tr>
<td>Academic Division</td>
<td>15</td>
<td>10</td>
</tr>
<tr>
<td>Health System</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>College at Wise</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>
Report to BOV ACR Committee: September 2016 Audit Department Status

Our audit findings and management’s related action plans are tagged with a risk classification to enable analysis of overall trends in processes and controls. We summarize risks into Compliance, Operational, and Fraud/Waste/and Abuse categories, with additional subcategories as below:

### Action Plans by Operational Risk Subcategories

<table>
<thead>
<tr>
<th>Category</th>
<th>FY 2017</th>
<th>FY 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>Efficiency and Effectiveness</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>Key Financial Controls</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Student Experience</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>General IT Controls*</td>
<td>1</td>
<td>8</td>
</tr>
</tbody>
</table>

### Action Plans by Compliance Risk Subcategories

<table>
<thead>
<tr>
<th>Category</th>
<th>FY 2016</th>
<th>FY 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>UVA Policies &amp; Procedures</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>Regulatory Compliance</td>
<td>6</td>
<td>0</td>
</tr>
</tbody>
</table>

**Audit Department Creates Value Through Focus On:**

- Leadership and Relationship Acumen
- Industry and Technical Competence
- Efficiency and Effectiveness of Audit Process
- Relevance to Risks that Matter Most
Report to BOV ACR Committee: September 2016 Audit Department Status

APPENDIX

<table>
<thead>
<tr>
<th>Priority 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>A Priority 1 item signifies a control and/or process deficiency of sufficiently high risk that it provides minimal or no assurance that institutional objectives will be achieved. Management must take immediate corrective action to mitigate Priority 1 deficiencies.</td>
</tr>
</tbody>
</table>

Open Priority 1 Action Plans:

Three Priority 1 action plans related to matters reported in the Curry School of Education audit report of June 30, 2016, remain open:

The finding related to incomplete and/or inconsistent published degree materials required 2 separate corrective actions from:

1. University Registrar
2. Curry School

The planned implementation date for the third open action plan, oversight of internal controls compliance via the Internal Controls Questionnaire process performed by the Comptroller’s office, has also been extended.

Progress toward closure of the issues is being made; implementation dates have been extended from those originally identified by management. We will update the Audit, Compliance, and Risk Committee on action plan implementation at the upcoming December 2016 meeting.
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: September 16, 2016

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: III.B. University Compliance: Medical Center Compliance and Privacy Office Staffing Report

ACTION REQUIRED: None

BACKGROUND: Mr. Gary Nimax, Assistant Vice President for Compliance, will report on the search for the Medical Center’s new Compliance and Privacy Officer.

A national search is underway to fill the vacant position on a permanent basis. Mr. Nimax will provide an update on the status of the search and a timeline for completion.
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: September 16, 2016

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: III.C. Enterprise Risk Management (ERM) Report

ACTION REQUIRED: None

BACKGROUND: Mr. James Matteo, Associate Vice President and Treasurer, will report on actions taken toward accomplishing the three key priorities for the ERM program, as first identified at the Committee's February 2016 meeting. The effort consists of three near-term priorities designed to: (1) reposition and enrich the program; (2) enhance board reporting; and (3) onboard ERM at the Health System.

Actions have been taken to reposition the program, including the adoption of an Enterprise Risk Management Charter and the formation of a Risk Management Council to provide guidance in support of the effort. Risk Management Networks, comprised of representatives from major business units, have been formed in both the Academic Division and Health System. These networks help identify inherent and emerging risks, serve as a connection between executive-level and department risk management activities, and seek to raise risk awareness among units across the University.

Work is underway to update the key risk list with an increased focus on aligning risks with strategy and major objectives. We are currently working with the Chair of the Committee to finalize the format, content, and frequency of a new reporting approach. We project having that reporting completed for the December 2016 Committee meeting.

Significant efforts have been made to onboard the Health System. Under the new framework, we began this effort by first identifying the major strategies and objectives of the health system. An inaugural risk management network has been formed and efforts are underway to identify key risks to the Health System's achievement of its goals.