AUDIT, COMPLIANCE, AND RISK COMMITTEE
(Open Session)

Friday, June 10, 2016
1:15 – 2:00 p.m.
Auditorium of the Albert & Shirley Small
Special Collections Library, Harrison Institute

Committee Members:
Frank E. Genovese, Chair  John G. Macfarlane III
Mark T. Bowles  Jeffrey C. Walker
L.D. Britt, M.D.  William H. Goodwin Jr., Ex-officio
Frank M. Conner III  Adelaide Wilcox King, Faculty
Consulting Member

AGENDA

I. REMARKS BY THE COMMITTEE CHAIR  1

II. CONSENT AGENDA
• Corporate Compliance and Privacy Office Project  2
  Schedule for Fiscal Year 2017 (Mr. Genovese)

III. COMMITTEE DISCUSSION
A. Auditor of Public Accounts (APA) Audit Entrance  8
  Meeting for Fiscal Year 2016 (Ms. Melody Bianchetto
  to introduce Mr. Eric M. Sandridge; Mr. Sandridge
  to report)
B. Audit Department Activities Report (Ms. Carolyn Saint)  9
C. University Compliance: Medical Center Compliance and  12
  Privacy Office Staffing Report (Mr. Genovese
  to introduce Mr. Gary S. Nimax; Mr. Nimax to report)
D. Enterprise Risk Management (ERM) Program Report  13
  (Mr. Genovese to introduce Mr. James Matteo; Mr.
  Matteo to report)

IV. CLOSED SESSION
• Evaluation of the performance of specific personnel,
  consultation with legal counsel, and discussion of
  security-related matters and Medical Center operations as
  provided for in Section 2.2-3711(A)(1), (7), (19) and (22)
  of the Code of Virginia.

1
BOARD MEETING: June 10, 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. CORPORATE COMPLIANCE AND PRIVACY OFFICE PROJECT SCHEDULE FOR FISCAL YEAR 2017: Approves the schedule for the Corporate Compliance and Privacy Office for Fiscal Year 2017

Ms. Annette Norton, Interim Chief Compliance and Privacy Officer for the Medical Center, has proposed the attached Corporate Compliance and Privacy Office Project Schedule for the fiscal year 2017. The schedule has been developed based on required work from federal, state, and other regulatory agencies, risk assessment models, requests from Medical Center management, and analyses of work performed in prior years.

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

<table>
<thead>
<tr>
<th>CORPORATE COMPLIANCE AND PRIVACY OFFICE PROJECT SCHEDULE FOR FISCAL YEAR 2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESOLVED, the Corporate Compliance and Privacy Office Project Schedule for the Medical Center for fiscal year 2017 is approved as recommended by the Audit, Compliance, and Risk Committee.</td>
</tr>
</tbody>
</table>
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM

UVA Medical Center
Corporate Compliance and Privacy Office Project Schedule FY 2017

Determination of Hours Available for 2016-2017
Corporate Compliance and Privacy Projects

<table>
<thead>
<tr>
<th>Fiscal Year (FY) 2017</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Hours Available</td>
<td>8,840</td>
</tr>
<tr>
<td>Less: Vacancies</td>
<td>2,080</td>
</tr>
<tr>
<td>Sub-Total</td>
<td>6,760</td>
</tr>
<tr>
<td>Professional Development</td>
<td>325</td>
</tr>
<tr>
<td>Leave and Holidays</td>
<td>860</td>
</tr>
<tr>
<td>Other Activities: Office and Personnel Administration, Committee Meetings</td>
<td>320</td>
</tr>
<tr>
<td>Hours Available for Corporate Compliance and Privacy Projects</td>
<td>5,255</td>
</tr>
</tbody>
</table>

The schedule above outlines the available staff resources for the Corporate Compliance and Privacy Office (Office). The schedule is developed based on required work from federal, state, and other regulatory agencies, risk assessment models, requests from Medical Center management, and analyses of work performed in prior years. The hours available for Corporate Compliance and Privacy projects have been reduced (by 2,080 hours/1 FTE) due to the vacancy of the Chief Corporate Compliance and Privacy Officer. This schedule will be readjusted after that position has been filled on a permanent basis.

The Office staff consists of the following positions:

- Chief Corporate Compliance and Privacy Officer – currently vacant (0 hours)
- Interim Corporate Compliance and Privacy Officer / Program Coordinator (2080 hours)
- Compliance and Privacy Senior Analyst (2080 hours)
- Compliance and Privacy Analyst (2080 hours)
- Compliance and Privacy Specialist (25% of full time position – 520 hours)

The schedule includes hours allocated for professional development activities. During FY17, Office staff plan to attend the Society of Corporate Compliance and Ethics Basic Compliance and Ethics Academy, the Fairwarning Ready Certified Professionals Training Program, the Health Care Compliance Association Compliance Institute and the Enforcement Compliance Institute, and relevant webinars and/or other educational sessions for professional development. These professional development activities are vitally important and provide the Office an opportunity to network with other compliance and privacy professionals; obtain information on
emerging issues; and gain knowledge on issues that compliance and privacy professionals encounter daily.

Hours for other activities related to the Office include serving on relevant committees throughout the Medical Center. The Interim Compliance and Privacy Officer will continue to attend such meetings to determine if the Office provides added value. These hours also include the time allotted to review the annual Office of the Inspector General (OIG) Work Plan and solicit feedback from Management regarding the risks identified by the OIG that apply to our setting. This document and related communications are used to determine the Office’s scheduled projects.

After removing hours for professional development, leave and holidays, and other activities, there are 5,255 hours remaining for Corporate Compliance and Privacy Office projects.

| Allocation of Hours Available for Corporate Compliance and Privacy Projects |
|------------------|-----------|
| Fiscal Year 2017 | HOURS    |
| Hours Available for Corporate Compliance and Privacy Projects | 5,255 |
| Consulting: Policy and Procedure Reviews, Guidance | 700 |
| Developing and Conducting Training: Department Specific Training, Website Documents, Communications | 265 |
| Unscheduled Compliance Projects: Federal or State Agency Investigations, Auditing and Monitoring, Management Requests, Industry Alerts, Investigations | 1,000 |
| Hours Available for Corporate Compliance and Privacy Scheduled Projects | 2,200 |

The Office promptly responds to and investigates issues of suspected violations related to compliance and privacy. Inappropriate, but accidental, disclosures of protected health information comprise a large number of the privacy investigations. Each of these accidental disclosures is assessed to determine if the incident is a reportable breach (i.e., when a patient is provided with another patient’s protected health information). The hours allocated to this function are included in unscheduled privacy projects.

The University of Virginia Health System’s Notice of Privacy Practices was last reviewed and updated in 2013. This document will be reviewed this fiscal year and any applicable and relevant changes will be made. The hours allocated to this review are included in unscheduled privacy projects.
Developing and conducting training accounts for approximately 965 hours (18%) of the Office’s work hours. Special and unscheduled projects account for approximately 2,090 hours (40%) of the Office’s work hours.

Corporate Compliance and Privacy Projects
Scheduled Projects

<table>
<thead>
<tr>
<th>Fiscal Year 2017</th>
<th>HOURS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outpatient Clinic or Procedure Area Audits (e.g., coding, billing and/or documentation review related to medications, procedures, facility fees, or others)</td>
<td>600</td>
</tr>
<tr>
<td>Privacy Auditing and Monitoring: Monthly Site Visits and Medical Record Audits</td>
<td>400</td>
</tr>
<tr>
<td>Inpatient Medicare Severity Diagnosis Related Groups Audits (e.g., coding, billing and/or documentation review related to correct coding validation, medical necessity, hospital acquired conditions, or others)</td>
<td>800</td>
</tr>
<tr>
<td>Developing and Conducting Training: New Hire and Annual Compliance and Privacy Training, Hybrid Privacy Training</td>
<td>400</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>2,200</strong></td>
</tr>
</tbody>
</table>

The hours allocated above for work related to privacy and training have not been reduced due to the staff vacancy because of the importance of these activities to the Medical Center. The Office provides content for compliance and privacy-related topics for the mandatory new hire and retraining modules each year. The content is based on trends observed through risk assessments, auditing and investigations; law and regulatory changes; and industry needs. In addition, the Office provides additional training as requested from departments. The Office regularly participates and presents at the Housestaff Orientation.

In order to avoid duplication of resources, and a desire to participate in a partnership across the continuum of compliance-related departments, the Office meets regularly with the University’s Chief Audit Executive and staff and the University Physicians Group Director for Audit and Compliance and staff, in order to coordinate and work together to assure that the Health System’s risk are appropriately addressed. During these meetings, ongoing and anticipated projects are discussed.

The fully detailed project schedule has not yet been determined; however, there are two industry-specific high-risk areas that will be assessed:

- The 340B Pharmacy Drug Pricing Program continues to be a high risk area, due to the complexity of the requirements, regulatory scrutiny, and high dollar volume. The Medical
Center Pharmacy staff has policies and procedures in place to ensure compliance with the Program. Our Office will review their policies and procedures and audit plan to assure that they are in compliance with the Program.

- The Centers for Medicare and Medicaid Services' Two-Midnight Rule continues to be a highly-audited billing rule. This Rule originated from the Recovery Audit program when CMS identified high rates of error for hospital services rendered in a medically-unnecessary setting (i.e., inpatient rather than outpatient.) The Office has conducted a thorough review within the past two years, and will continue to review the necessity of inpatient vs. observation status with each inpatient billing review the Office completes.

The Office will continue its seamless working relationship with Health Information Technology on some key emerging risk areas such as cybersecurity, the security and process of texting patient information, and cloud computing safe and secure initiatives. There is growing concern among the industry on the security and protection of the data stored on medical devices. This topic was contained in the 2015 OIG Work Plan where the OIG reported that computerized medical devices such as dialysis machines, radiology systems, and medication dispensing systems that are integrated with electronic medical records (EMRs) pose a growing threat to the security and privacy of personal health information. The OIG said they will determine whether hospitals' security controls over networked medical devices are sufficient to effectively protect associated electronically protected health information (ePHI) and ensure beneficiary safety. The Office will gather best practices and standards from throughout the industry, and provide that information to Health Information Technology for their review.

Some additional Office-related activities that are planned for this fiscal year, and will require the need for significant resource hours, are the implementation and go-live of the MD Audit Compliance Software. This software will be used to support sampling, complete root cause analysis, and identify and reduce compliance billing risks. Additionally, the Office will pursue ways to reduce the use of paper in the Office in order to be in line with the University of Virginia’s Sustainability Plan; to be better stewards of the environment; and resolve the lack of space for filing of documents in the Office. The Office is investigating solutions that will allow for scanning documents in to a database and the electronic storage of older files.

Scheduled projects account for approximately 2,200 hours (42%) of the Office’s scheduled work hours.
AGENDA ITEM SUMMARY

BOARD MEETING: June 10, 2016

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: III.A. Auditor of Public Accounts (APA)
Audit Entrance Meeting for Fiscal Year 2016

ACTION REQUIRED: None

BACKGROUND: The APA meets with the Audit, Compliance, and Risk Committee as an initial step in the completion of the University's annual financial statement audit. Mr. Eric M. Sandridge, the APA's project manager for the FY 2016 audit, will highlight the work of the APA during the current audit. This does not require formal action, but is information of which the Board should be made aware.

Eric M. Sandridge is the Director of Higher Education Programs for the Virginia Auditor of Public Accounts and has served in that position since 2012. His responsibilities include management of the office's Higher Education Programs Specialty Team and project management oversight for audits of various agencies and institutions of the Commonwealth. Eric has served as audit
director for the Virginia Community College System, Old Dominion University, Virginia Commonwealth University, Norfolk State University, University of Virginia, and the Department of Alcoholic Beverage Control annual audits.

He also coordinates required federal audits at the Commonwealth's institutions of higher education, which support Virginia's statewide single audit report. He received his B.B.A. in Finance from the College of William and Mary and is a Certified Public Accountant and a Certified Government Financial Manager.
UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: June 10, 2016

COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: III.B. Audit Department Activities Report

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 2016.

FY 2016 Highlights

Audit Team: Rebuilt and Stabilized the Team
• Hired and on-boarded 3 audit directors.
• Hired and on-boarded seasoned IT security professional as Senior IT Auditor
• Team completed skills self-assessment as foundation to training and development plan

Audit Operations: Risk Based, Strategically Relevant Audit Approach
• Created data-driven audit risk universe and plan, relevant to strategic objectives and ERM risks
• In design phase of 2 forward-thinking methodologies relevant to our decentralized environment: Integrated Assurance (an assessment of compliance risk management effectiveness) and Fiscal Stewardship (data-driven analysis of internal controls)

• Completed comprehensive compliance risk assessment (attorney client privileged) in partnership with AVP for Compliance and General Counsel

• Implemented new audit reporting template to include audit finding prioritization, improved executive summaries, management’s responses

• Began tagging audit findings with relevant risks to enable enhanced board and management reporting
## Audit Projects FY 2016

<table>
<thead>
<tr>
<th>Project Description</th>
<th>Completed</th>
<th>In Progress</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procurement</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Outpatient Charge Capture (Univ. Med. Assoc.)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Presidential Travel</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Pyxis System Access</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>General Ledger Transfers</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Curry School of Education</td>
<td></td>
<td>X Report Draft</td>
</tr>
<tr>
<td>Distributed IT Systems Current State Assessment</td>
<td></td>
<td>X Report Draft</td>
</tr>
<tr>
<td>Epic Phase 2 Implementation Project Health Check</td>
<td>X First Checkpoint Report Issued</td>
<td>X</td>
</tr>
<tr>
<td>Integrated Assurance:(Attorney Client Privileged)</td>
<td>X Compliance Risk Assessment Completed</td>
<td>X</td>
</tr>
<tr>
<td>Fiscal Stewardship: Using data analytics to identify metrics for key risk indicators</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>System Security: Privileged Access</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Ivy Cloud Security and Governance</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>FY15 year-end inventory procedures (MC and Univ)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>OSIG hotline investigations</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
COMMITTEE: Audit, Compliance, and Risk

AGENDA ITEM: III.C. 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 staffing related to the Medical Center's Compliance and Privacy Office.

On April 28, 2016 Ms. Annette Norton began her role as the Interim Compliance and Privacy Officer at the Medical Center. Annette has been with the Corporate Compliance and Privacy Office since 2005. Annette is working in this interim role to replace Lori Strauss, who accepted a position as the Chief Compliance Officer at Stony Brook Medicine in New York.

A national search is underway to fill the position on a permanent basis. Mr. Nimax will provide an update on the status of the search and a timeline for completion.
BOARD MEETING: June 10, 2016

COMMITTEE: Audit, Compliance, and Risk

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

ACTION REQUIRED: None

BACKGROUND: At the Board’s February 2016 meeting, Mr. James Matteo, Associate Vice President and Treasurer, presented a plan to reposition and enrich the University’s ERM effort. The effort consists of three near-term priorities: (1) reposition and enrich the program, (2) enhance board reporting, and (3) onboard ERM at the Health System.

DISCUSSION: Mr. Matteo will report on the progress made around the near-term ERM priorities and present a timeline for completion. Significant steps in repositioning the program have already occurred including approval of the ERM Charter by the Board, launching the Risk Management Council, and updating the ERM framework. In addition, the risk governance architecture has been updated to reflect the various entities playing key roles in the ERM effort.

Over the coming months work will include: (1) updating the University’s list of key risks, which were last updated in 2014, (2) preparing a new board reporting format and package, and (3) continuing work with the health system to formalize and integrate their risk management program with that of the University. At the time when the University first launched its ERM effort, it was decided that the Health System would be excluded. We are now looking to integrate ERM efforts at both the Academic Division and the Health System.