UNIVERSITY OF VIRGINIA
BOARD OF VISITORS
MEETING OF THE
AUDIT AND COMPLIANCE
COMMITTEE
FEBRUARY 21, 2014

AUDIT AND COMPLIANCE COMMITTEE
(Open Session)

Friday, February 21, 2014
8:30 a.m. – 9:30 a.m.
Board Room, The Rotunda

Committee Members:

Hunter E. Craig, Chair	
Frank B. Atkinson	John L. Nau III
Kevin J. Fay	Linwood H. Rose
Frank E. Genovese	George Keith Martin, Ex-officio
Victoria D. Harker	Adelaide Wilcox King, Faculty
Bobbie G. Kilberg	Consulting Member

AGENDA

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: February 21, 2014

COMMITTEE: Audit and Compliance

AGENDA ITEM: I.A. Auditor of Public Accounts (APA) Audit and Management Letter

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 her findings. Ms. Deily will introduce Ms. Karen Helderman, who will report on behalf of that office. University management will then respond to the Auditor of Public Accounts' Audit and Management Letter. A summary of the Financial Statement Audit is attached.

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: February 21, 2014

COMMITTEE: Audit and Compliance

AGENDA ITEM: I.B. Institutional Response to APA Audit and Management Letter

ACTION REQUIRED: None

BACKGROUND: Mr. Pat Hogan, Executive Vice President and Chief Operating Officer, will present the institutional response to the Auditor of Public Accounts Audit and Management Letter. This report does not require formal action, but is information of which the Board should be made aware.

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: February 21, 2014

COMMITTEE: Audit and Compliance

AGENDA ITEM: I.C. Corporate Compliance and Privacy Office Status Report for Fiscal Year 2013 – 2014

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 2013-14

Projects	Scheduled	In Process (%)	Completed (%)
Outpatient Department Coding, Billing, and Documentation	2	1 (50%)	0 (0%)
Privacy Monitoring and Auditing	36	3 (8%)	18 (50%)
Inpatient Medicare Severity Diagnosis Related Groups Coding, Billing and Documentation	2	2 (100%)	0 (0%)
Total	40	6 (15%)	18 (45%)

Of 40 scheduled projects, 18 projects (45%) are complete and six projects (15%) are in process. During the first two months of this fiscal year, the Office had a staff analyst vacancy and the senior analyst had been in her position for only six months; therefore, due to the associated learning curves and training needs for new employees, we anticipate having all scheduled projects in process, and – ideally - completed, by the end of the fiscal year.

OTHER PROJECTS

Training: The Office reviewed and updated the Corporate Compliance new hire mandatory training module and the compliance and privacy content for the mandatory retraining module. The revised content provided education on trends or issues that were identified during site visits, through questions from staff or management, and through 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; and the need to use proper safeguards when transporting documents.

The Office provided six department-specific privacy presentations for five locations (KCRC, Community Medicine, 4 East, Student Health, and Outpatient Surgery Center). Fourteen hybrid departments identified as part of the Medical Center's covered entity and in need of training 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 for 27 employees.

With the required change from International Classification of Diseases, 9th Revision (ICD-9) to 10th Revision (ICD-10), on October 1, 2014, the Office is undergoing extensive training, as are others in the organization, to be ready for this new coding system. The compliance projects done within the office require knowing and applying the new coding system to ensure that documentation supports the codes and that the correct codes are submitted on the claims. All of the Office's professional staff must complete approximately 200 online training modules that take between 15 minutes and several hours to complete per module.

Consulting: The Office is consulted regularly by staff, management, clinicians, and others. These contacts include requests to locate regulations, provide input on Medical Center policy and procedure revisions impacting compliance and privacy, clarify policies and procedures related to such things as gifts or accessing medical records, conduct privacy audits and site reviews, and provide guidance on questions such as acceptable privacy practices.

Office personnel serve on several committees to provide guidance on compliance and privacy related issues. Some of these committees are the Grievance Committee, Joint Commission Steering Committee, Health Information Management Committee, Medical Center Management Group, Operations Leadership Committee, Payor Audit Review Committee, Security Oversight Committee, and several ICD-10 committees.

Notice of Privacy Practices: As a result of the federal Omnibus Final Rule that became effective September 23, 2013, the Office updated the University of Virginia HIPAA Notice of Privacy Practices (Notice) to be compliant with the changes in the Final Rule. This also required having the updated Notice translated to Spanish, reprinting and replacing the poster-sized Notice in all locations, removing and replacing the paper Notice in all areas, and educating staff on changes and the process for replacement.

The Notice describes the privacy practices of the University of Virginia Health System, including the Medical Center, Continuum Home Health Care and Infusion Services, the University Physicians Group, the Transitional Care Hospital, UVA Imaging Center, UVA Community Medicine, and the Virginia Urologic Foundation, as well as health care professionals, employees, volunteers, and students.

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: February 21, 2014

COMMITTEE: Audit and Compliance

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

ACTION REQUIRED: None

BACKGROUND: Beginning in 2008, the University conducted an initial assessment of the current framework for assessing and managing the University's strategic and high-level operational risks.

At the November 2013 meeting, Gary Nimax, the Assistant Vice President for Compliance and Enterprise Risk Management, reviewed the university's ERM program with the board and discussed related goals for fiscal year 2013-14.

The University has begun updating its risk register given the turnover in senior administration and board members, new strategic plan, internal financial model, and changes in higher education.

DISCUSSION: At the February 2014 meeting, Mr. Nimax will review a proposed survey instrument to be used to assist in the identification of the University's top risks in the academic division.

The proposed survey includes a list of specific risks to rate, summarized from the key risks identified by our prior ERM project, and other potential risks related to topics the board has discussed recently. Each survey recipient will be asked to indicate a rating for the potential impact to the University of each risk, as well as the likelihood of each risk occurring.

At the June 2014 meeting, we will review the results of the survey and the related mitigation strategies for the University's key risks.

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: February 21, 2014

COMMITTEE: Audit and Compliance

AGENDA ITEM: I.E. Audit Department Status Report for Fiscal Year 2013 – 2014

ACTION REQUIRED: None

BACKGROUND: Ms. Deily 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 2013-14 Audit Projects
as of December 31, 2013

Scheduled Audit Projects

	University	Hospital & IT	Internal Control Compliance	TOTAL
Scheduled	12*	13	3	28
Completed	4	5	1	10
% Completed	33%	38%	33%	36%
In Process	4	6	1	11
% In Process	33%	46%	33%	39%
% Complete or In Process	66%	84%	66%	75%

* Adjusted for vacancy. One project has been deferred to fiscal year 2014-15.

Non-Scheduled Projects

	University	Hospital & IT	Internal Control Compliance	TOTAL
Carry-forward	10	0	0	10
New	9	1	0	10
Total	19	1	0	20
Completed	10	1	0	11
% Completed	53%	100%	0%	55%
In Process	9	0	0	9
% In Process	47%	0%	0%	45%
% Complete or In Process	100%	100%	100%	100%

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: February 21, 2014

COMMITTEE: Audit and Compliance

AGENDA ITEM: I.F. Summary of Audit Findings

ACTION REQUIRED: None

BACKGROUND: Ms. Deily will present a summary of audit findings on the following audit reports: Health System Data Center, University Information Technology Risk Management, and Health System Information Technology Risk Management.

Health System Data Center **August 15, 2013**

BACKGROUND

The Health System (HS) has one main data center and three computer rooms that are located in different buildings with close proximity to each other providing highly reliable redundancy and fail-over for critical medical systems. The HS Operations team controls and monitors the data center, computer rooms and their systems on a 24x7 basis year round. A data center has numerous inherent risks. Inadequate physical and environmental security may leave equipment and information located within the data center unprotected from unauthorized access and environmental hazards which could lead to disruption of mission critical systems and services. Inadequate access management and controls may result in unauthorized or inappropriate access and changes. Last, but not least, lack of Business Continuity and Disaster Recovery Planning could result in extended or unrecoverable disruption of mission critical services in the event of a disaster or emergency.

AUDIT OBJECTIVES

Audit objectives included reviews of data center strategic planning and management; policy, standards, and procedures; access management; physical and environmental security management and controls; change management; third party service provider management; backup management; incident management; and business continuity and disaster recovery planning.

OPINION ON AUDIT OBJECTIVES

Overall, management of the Health System data center and related general controls appeared fairly stringent. We noted that an interdepartmental agreement (e.g. service level agreement (SLA) or memorandum of agreement (MOU)) did not exist with UVA Facilities to define data center specific service and maintenance requirements.

AREA NOTED FOR IMPROVEMENT

A list of data center specific maintenance, security and safety requirements was not documented in a performance agreement with UVA facilities to support monitoring and management of compliance.

MANAGEMENT'S RESPONSE

Management concurs and has agreed to address the identified condition.

IMPACT TO THE UNIVERSITY

The impact of proper security surrounding data centers and related general controls is always important in the Health System environments because of the following concerns:

- **Availability of mission critical systems, operations, and services;**
- **Public relations issues;**
- **HIPAA/FERPA/PCI non-compliance;**
- **Monetary damages as a result of lawsuits related to disclosure of sensitive or critical data; and**
- **Financial loss as a result of server down time and hours spent in repair or recovery as a result of intentional or unintentional damage done by individuals having improper access.**

University IT Risk Management **October 2, 2013**

BACKGROUND

The University manages information technology (IT) and security related risk through two primary documentation processes; the Information Technology Security-Risk Management (ITS-RM) and Mission Continuity Plan/Disaster Recovery Plan (MCP/DRP) documents. The Information Security Program and Records Office (ISPRO) was assigned both collection and administrative management of the processes to develop and maintain these documents. The management processes related to maintaining ITS-RMs and MCP/DRPs are important to ensure proper identification and assessment of IT and security risk and definition of disaster recovery plans and operating procedures. This audit focused on the management of ITS-RM and MCP/DRP documents among the University departments and schools.

AUDIT OBJECTIVES

Audit objectives included review of the University's ITS-RM and MCP/DRP format and contents, related policies, standards, and procedures (PSP), and document management processes. In conducting our work we reviewed the University departments' and schools' ITS-RM and MCP/DRP documents submitted to ISPRO. We did not review the Continuity of Operations Plan (COOP); that plan mostly focuses on personnel safety and was outside the scope of information technology.

OPINION ON AUDIT OBJECTIVES

The University's management of ITS-RM and MCP/DRP required improvement. Opportunity was noted to improve related policies, standards, and procedures and to further secure the submission of these documents to ISPRO.

AREAS NOTED FOR IMPROVEMENT

1) **ITS-RM and MCP/DRP related policies, standards, and procedures required improvement to address remediation guidelines for identified risks in the ITS-RM, required contents in MCP/DRP, and requirements for regular testing of the MCP/DRP.**

2) **Submissions of ITS-RM and MCP/DRP documents were not secured (e.g., encrypted).**

MANAGEMENT'S RESPONSE

Management concurs and has agreed to correct the identified conditions.

FINANCIAL IMPACT

The impact of proper ITS-RM and MCP/DRP is important in the University environments because of the following concerns:

- Unidentified risks may exist or inadequate risk mitigation may occur;
- Public relations issues may occur;
- HIPAA/FERPA/PCI compliance may be impacted; and
- Financial losses may be incurred due to the inability to operate and recover after a disaster.

BACKGROUND

UVA manages their information technology (IT) and security related risk through two primary documentation processes; the Information Technology Security-Risk Management (ITS-RM) and Business Continuity Plan/Disaster Recovery Plan (BCP/DRP) documents. The Information Security Program and Records Office (ISPRO) was assigned both collection and administrative management of the processes to develop and maintain these documents. The management processes related to maintaining ITS-RMs and BCP/DRPs are important to ensure proper identification and assessment of IT and security risk and definition of disaster recovery plans and operating procedures.

AUDIT OBJECTIVES

Audit objectives included review of the Health System's ITS-RM and BCP/DRP format and contents, related policies, standards, and procedures (PSP), and document management processes. Audit work performed focused on reviewing the Health System's ITS-RM and BCP/DRP documents submitted to Information Security, Policies and Records Office (ISPRO). We also reviewed BCP/DRP documents maintained within the data center for currency and completeness. We did not review the Continuity of Operations Plan (COOP); that plan mostly focuses on personnel safety and was outside the scope of information technology.

OPINION ON AUDIT OBJECTIVES

In general, the Health System ITS-RM and BCP/DRP appeared adequate to manage risk and business continuity and disaster recovery planning. Some minor (verbal) issues were noted related to improving the keyword search function for PSP and improved options for submitting the ITS-RM and BCP/DRP documents. Health System management was receptive to our verbal comments and suggestions.

MANAGEMENT'S RESPONSE

Management concurs and has agreed to address our suggestions.

FINANCIAL IMPACT

The impact of proper ITS-RM and BCP/DRP is important in the University environments because of the following concerns:

- **Unidentified risks may exist or inadequate risk mitigation may occur;**
- **Public relations issues may occur;**
- **HIPAA/FERPA/PCI compliance may be impacted; and**
- **Financial losses may be incurred due to the inability to operate and recover after a disaster.**

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: February 21, 2014

COMMITTEE: Audit and Compliance

AGENDA ITEM: III. Approval of the Summary by the Auditor of Public Accounts, the 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, the findings of the Auditor of Public Accounts, and a summary of recent internal audit findings.

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

APPROVAL OF THE SUMMARY OF COMPLIANCE FINDINGS, THE AUDITOR OF PUBLIC ACCOUNTS FINDINGS, AND THE SUMMARY OF INTERNAL AUDIT FINDINGS

RESOLVED, the Summary of Compliance Projects for the period July 1, 2013 through December 31, 2013, as presented by the Chief Corporate Compliance and Privacy Officer, the Auditor of Public Accounts Findings for fiscal year 2012-2013, and the Summary of Internal Audit Findings for the period October 1, 2013 through December 31, 2013, as presented by the Chief Audit Executive, are approved.

ATTACHMENT

University of Virginia
Results of Financial Statement Audit
For the Year Ended June 30, 2013 **Attachment 1**

Area	Comments
Auditor's Opinion	We have issued an unqualified opinion on the University's financial statements for the year ended June 30, 2013. Our opinion is included in the University's fiscal year 2013 Financial Statement Report.
Scope of Internal Control Work	We have also issued a separate report on Internal Controls and Compliance that was distributed to the Board of Visitors. We obtained a sufficient understanding of internal control to plan our audit and to determine the nature, timing, and extent of testing performed. Our audit identified four matters that we consider to be significant deficiencies, but not material weaknesses in internal control.
Compliance Testing	We found no instances of noncompliance that are required to be reported.
Fraud and Illegal Acts	We found no indications of fraudulent transactions or illegal acts.
Significant Audit Adjustments	All audit adjustments were reviewed with management and recorded in the audited financial statements.
Accounting Policies, Principles, Methods, and Estimates	• We concur with management's application of accounting principles. • We reviewed the basis for accounting estimates and these estimates appear to be reasonable based on available information and consistent with prior periods. • There were no material changes to accounting and reporting policies and standards during the year. • There were no material alternative accounting treatments identified as a result of the audit. • There were no unusual transactions or significant accounting policies in controversial or emerging issues. • There were no disagreements with management about auditing, accounting, or disclosure matters.

NCAA Agreed-Upon Procedures

We also performed an agreed-upon engagement to assist the University in complying with NCAA Bylaw 3.2.4.16.1. All adjustments that we identified were properly corrected in the Schedule. Our separate report on this Agreed-upon Procedures engagement has been distributed to the Board of Visitors.