

**UNIVERSITY OF VIRGINIA
BOARD OF VISITORS
MEETING OF THE
AUDIT COMMITTEE
January 31, 2003**

AUDIT COMMITTEE
(Open Session)

Friday, January 31, 2003
9:15 - 9:45 a.m.
Board Room, The Rotunda

Committee Members:

Elizabeth A. Twohy, Chair Warren M. Thompson
Terence P. Ross John P. Ackerly, III, Ex Officio

AGENDA

	<u>PAGE</u>
• INFORMATION REPORT (Ms. Deily)	
A. Auditor of Public Accounts (APA) Audit and Management Letter (Ms. Deily to introduce Mr. Walter Kucharski; Mr. Kucharski to report)	1
B. Health System Response to the APA Audit and Management Letter (Ms. Deily to introduce Ms. Barbara Baldwin, Chief Information Officer for the Medical Center, Ms. Baldwin to report)	2

UNIVERSITY OF VIRGINIA
BOARD OF VISITORS AGENDA ITEM SUMMARY

BOARD MEETING: January 31, 2003

COMMITTEE: Audit

AGENDA ITEM: Information Report

ACTION REQUIRED: None

BACKGROUND: The Auditor of Public Accounts of the Commonwealth conducts an annual audit of the University and the Health System and reports to the Board at the January meeting on his findings. Ms. Deily will introduce the Auditor, Mr. Walter Kucharski, who will report. The Health System will respond to the Auditor's Audit and Management letter.

HEALTH SYSTEM DIVISION

Recommendation: Continue Security Initiative Over Critical Information Systems and Network

The Health Systems Computing Services (HSCS) continues its initiative to enhance security over the Health System's network of information systems. As custodian over data resources that are vital to the Health System's operations, HSCS must implement and maintain strong security controls that adequately safeguard the Health System's information resources and, as importantly, protect the privacy of its patients. The Federal Health Insurance Portability and Accountability Act's Privacy Rule, effective April 2003, heightens awareness of the need for strong information security policies and procedures along with accountability of staff accessing patient information.

To increase security within the entire information systems environment, management developed a comprehensive security strategy. Initially management, with the aid of a security consultant, conducted a risk analysis and vulnerability assessment. The security consultant completed their assessment and made recommendations in May 2000.

The assessment addressed several vulnerabilities in the Health System's network security system. After correcting the most vulnerable network concerns, management began developing a comprehensive, ongoing information security program. The program encompasses the review and development of information security policies, development and administration of a new "more secure" network, and monitoring the access of sensitive data.

The new "more secure" network has been installed. The network includes improved physical security, enhanced authentication procedures, encryption of data communications for users outside the network, and stronger prevention of unauthorized network access from outside the Health System's network.

Health Systems Computing Services has begun moving its more than 5,000 network users to the new the secure clinical subnet. They will initially migrate the Medical Center, consisting of University Hospital, Primary Care Clinics, and West Hospital, by April 2003. Afterwards, remote centers such as Northridge, Orange, etc. will be migrated by the end of the calendar year.

HEALTH SYSTEM DIVISION, continued

Further, Health System management is conducting an ongoing review of policies in cooperation with the University's Department of Information Technology and Communication and under the direction of its Director of Information Services and Security. Also, the Health System's Corporate Compliance Office has begun a program monitoring staff access of patient data.

Management should continue with the development and implementation of the comprehensive, on-going information security program.

Management Response: Management concurs. The medical center, consisting of the University Hospital, Primary Care Clinics, and West Hospital, will be migrated to the secure clinical subnet by April 2003. Remote centers such as Northridge, Orange, etc. will be migrated as funding allows, by the end of the calendar year.