STATE OF NORTH CAROLINA

AUDIT OF THE INFORMATION SYSTEM GENERAL CONTROLS

AT

UNC HOSPITALS

CHAPEL HILL, NORTH CAROLINA

DECEMBER 2002

OFFICE OF THE STATE AUDITOR

RALPH CAMPBELL, JR.

STATE AUDITOR

AUDIT OF THE INFORMATION SYSTEM GENERAL CONTROLS

AT

UNC HOSPITALS

CHAPEL HILL, NORTH CAROLINA

DECEMBER 2002

STATE OF NORTH CAROLINA
Office of the State Auditor

Ralph Campbell, Jr.
State Auditor

2 S. Salisbury Street
20601 Mail Service Center
Raleigh, NC 27699-0601
Telephone: (919) 807-7500
Fax: (919) 807-7647
Internet http://www.osa.state.nc.us

AUDITOR'S TRANSMITTAL

The Honorable Michael F. Easley, Governor
Members of the North Carolina General Assembly
The Board of Directors of the University of North Carolina Hospitals
Mr. Eric B. Munson, President and CEO

Ladies and Gentlemen:

We have completed our information systems (IS) audit of UNC Hospitals. The audit was conducted in accordance with *Government Auditing Standards* and *Information Systems Audit Standards*.

The primary objective of this audit was to evaluate IS general controls at UNC Hospitals. The scope of our IS general controls audit included general security, access controls, program maintenance, systems software, systems development, physical security, operations procedures, help desk, and disaster recovery. Other IS general control topics were reviewed as considered necessary.

This report contains an executive summary that highlights the areas where UNC Hospitals has performed satisfactorily and where improvements should be made.

We wish to express our appreciation to the staff at UNC Hospitals for the courtesy, cooperation and assistance provided to us during this audit.

North Carolina General Statutes require the State Auditor to make audit reports available to the public. Copies of audit reports issued by the Office of the State Auditor may be obtained through one of the options listed in the back of this report.

Respectfully submitted,

Ralph Campbell, Jr.

Ralph Campbell, Jr.
State Auditor

[This Page Left Blank Intentionally]

TABLE OF CONTENTS

EXECUTIVE SUMMARY

We conducted an information system (IS) audit at UNC Hospitals from June 3, 2002 through August 30, 2002. The primary objective of this audit was to evaluate the IS general controls in place during that period. Based on our objective, we report the following conclusions.

General security involves the establishment of a reasonable security program that addresses the general security of information resources. We did not identify any significant weaknesses in general security controls of information resources.

The **access control** environment consists of access control software and information security policies and procedures. We reviewed the access controls for the UNC Hospitals mainframe and a UNIX server. We found several weaknesses in access controls. Due to the sensitive nature of the conditions found in the weaknesses, we have conveyed these findings to management in a separate letter pursuant to the provision of North Carolina G.S. 147-64.6(c)(18).

Program maintenance primarily involves enhancements or changes needed to existing systems. We found that application programmers have the ability to move and run programs in the Unix production environment. See Audit Finding 1, *Application programmers' access to the Unix production environment* for further information.

Systems software is the collection of programs that drive the computer. The selection of systems software should be properly approved and the software should be maintained by the computer center. We did not identify any significant weaknesses in systems software during our audit.

Systems Development includes the creation of new application systems or significant changes to existing systems. We did not identify any significant weaknesses in systems development during our audit.

Physical security primarily involves the inspection of the university's computer center for the controls that should reasonably secure the operations of the computer center from foreseeable and preventable threats from fire, water, electrical problems, and vandalism. We noted that employee access to computer room was not adequately restricted. See Audit Finding 2, *Employee access to the computer room* for further information.

The **operations procedures** of the computer center include all of the activities associated with running application systems for users. We did not identify any significant weaknesses in operations procedures during our audit.

The **Help Desk** function ensures that any problem experienced by a computer system user is appropriately resolved. We did not identify any significant weaknesses in the help desk operations during our audit.

A complete **disaster recovery** plan that is tested periodically is necessary to enable the Hospital to recover from an extended business interruption due to the destruction of the computer center or other Hospital assets. The Hospital does not have a disaster recovery plan in place. UNC Hospitals is currently working on a disaster recovery plan. See Audit Finding 3, *No disaster recovery plan* for further information. All backup tapes are not adequately stored off site. See Audit Finding 4, *Off-site storage of back-up tapes* for further information.

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Under the North Carolina General Statutes Chapter 147-64.6, the State Auditor is responsible for examining and evaluating the adequacy of operating and administrative procedures and practices, systems of accounting, and other elements of State agencies. This IS audit was designed to ascertain the effectiveness of general controls at UNC Hospitals.

SCOPE

General controls govern the operation and management of computer processing activities. The scope of our IS general controls audit was to review general security issues, access controls, program maintenance, systems software, systems development, physical security, operations procedures, helpdesk, and disaster recovery which directly affect UNC Hospitals computing operations. Other IS general control topics were reviewed as considered necessary.

METHODOLOGY

We audited policies and procedures, interviewed key administrators and other personnel, examined system configurations, toured the computer facility, tested on-line system controls, reviewed appropriate technical literature, reviewed computer generated reports, and used security evaluation software in our audit of application controls. We conducted our audit in accordance with the standards applicable to performance audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States and *Information Systems Audit Standards* issued by the Information Systems Audit and Control Association.[1]

1 In 1992 the State created the Information Resource Management Commission to provide statewide coordination of information technology resources planning. The IRMC provides state enterprise IT leadership including increased emphasis and oversight for strategic information technology planning and management; policy development; technical architecture; and project certification. Pursuant to North Carolina General Statute 147-33.78 numerous state officials serve on the IRMC including four members of the Council of State who are appointed by the Governor. The State Auditor has been appointed a member of the IRMC and elected as chair of the IRMC by its members.

[This Page Left Blank Intentionally]

BACKGROUND INFORMATION

UNC Hospitals opened in September 1952 under the name North Carolina Memorial Hospital. In May 1989, the N.C. General Assembly created the University of North Carolina Hospitals entity as a unifying organization to govern constituent hospitals and to project a modern and accurate identity for the hospitals of the University of North Carolina at Chapel Hill.

UNC Hospitals includes North Carolina Children's Hospital, North Carolina Memorial Hospital, North Carolina Neurosciences Hospital, and North Carolina Women's Hospital. In 2002, the N.C. Children's and Women's Hospitals moved to new state-of-the-art facilities designed to offer high-quality health care in a comfortable, family-friendly environment.

Computer processing for these hospitals is provided by UNC Hospitals' Information Services Division.

UNC Hospitals is a public, academic medical center operated by and for the people of North Carolina. The Hospitals' mission is to provide high quality patient care, to educate health care professionals, to advance research and to provide community service.

Each year UNC Hospitals cares for residents from all 100 counties in North Carolina and several surrounding states. About 30 percent of UNC Hospitals' patients come from Orange and surrounding counties.

[This Page Left Blank Intentionally]

AUDIT RESULTS AND AUDITEE RESPONSES

The following audit results reflect the areas where UNC Hospitals has performed satisfactorily and where recommendations have been made for improvement.

GENERAL SECURITY ISSUES

General security issues involve the maintenance of a sound security management structure. A sound security management structure should include a method of classifying and establishing ownership of resources, proper segregation of duties, a security organization and resources, policies regarding access to the computer systems and a security education program. UNC Hospitals has established a reasonable security program that addresses the general security of information resources. We did not identify any significant weaknesses in general security during our audit.

ACCESS CONTROLS

The access control environment consists of access control software and information security policies and procedures. An individual or a group with responsibility for security administration should develop information security policies, perform account administration functions and establish procedures to monitor and report any security violations. We reviewed the access controls for the UNC Hospitals mainframe and a UNIX server. We found several significant weaknesses in access controls. Due to the sensitive nature of the conditions found in the control weaknesses, we have conveyed these findings to management in a separate letter pursuant to the provision of North Carolina G.S. 147-64.6(c)(18).

PROGRAM MAINTENANCE

Program maintenance consists of making changes to existing application systems. Programmers should follow program change procedures to ensure that changes are authorized, made according to specifications, properly tested, and thoroughly documented. Application programmers should be restricted to a test environment to ensure that all changes to production resources are tested and approved before moving the changes into production. Changes to application system production programs should be logged and monitored by management.

AUDIT FINDING 1: APPLICATION PROGRAMMERS' ACCESS TO THE UNIX PRODUCTION ENVIRONMENT

Application programmers have the ability to move and run programs in the Unix production environment. As a result, unauthorized changes to programs and data could occur.

Senior Management should implement a division of roles and responsibilities which should exclude the possibility for a single individual to subvert a critical process. Management should also make sure that personnel are performing only those duties stipulated for their respective jobs or positions. In particular, a segregation of duties should be maintained between the system development maintenance function, the processing operations function and the user Organization. In addition, the security responsibility should be clearly separated from the processing operations function. When this is not possible, mitigating controls such as monitoring programmer access and appropriate supervisory review of this access should be established.

Recommendation: UNC Hospitals should establish procedures to limit application programmer access to the production environment, wherever possible, or implement a change control process that will enable programmer access to the production environment to be monitored.

Auditee's Response: ISD Management agrees with finding. In our environment, an affordable set of tools does not exist to allow production move-ups of programmer code by Production Control area. We will investigate implementing Data Set Auditing processes in conjunction with Security Administration Department.

SYSTEMS SOFTWARE

Systems software is the collection of programs that the computer center uses to run the computer and support the application systems. This software includes the operating system, utility programs, compilers, database management systems and other programs. The systems programmers have responsibility for the installation and testing of upgrades to the system software when received. Our audit did not identify any significant weaknesses in system software.

SYSTEMS DEVELOPMENT

Systems development includes the creation of new application systems or significant changes to existing systems. Systems development projects can be expensive and affect the operations of the agency in significant ways. Consequently, the agency should have a strategic or master plan for systems development. Each development project should be managed using project management techniques and should adhere to a clearly defined systems development methodology. When a project is completed, the finished product should include a

comprehensive set of documentation so that the users, operators and programmers each have the information they need to do their jobs. Our audit did not identify any significant weaknesses in systems development.

PHYSICAL SECURITY

Controls over physical security are designed to protect a computer center from service interruptions resulting from fire, water, electrical problems, vandalism, and other causes.

AUDIT FINDING 2: EMPLOYEE ACCESS TO THE COMPUTER ROOM

There is excessive employee access to computer room. Authorizing employee access to the computer room beyond an employee's need (based on their current job duties) increases the risk of disruption to computer service and also increases the risk of unauthorized access to data.

According to Control Objectives for Information Technology (COBIT), appropriate physical security and access control measures should be established for information technology facilities, including off-site use of information devices in conformance with the general security policy. Access should be restricted to individuals who have been properly authorized.

Recommendation: The operations manager should review the current access list to the computer room and modify the list to ensure that only employees that specifically need access to facility are granted access. The list should be reviewed periodically. All access approvals should be centrally approved.

Auditee's Response: ISD Management does agree that excessive employee access to Computer Room was granted. ISD Management has removed all personnel from access list except for Computer Operations Staff and Customer Support Center Staff (Help Desk) who are housed within Computer Room effective September 20, 2002.

OPERATIONS PROCEDURES

The operations of the computer center include all of the activities associated with running application systems for users. Procedures should be in place to control the scheduling and running of production jobs, restarting production jobs when problems occur, storing, handling and mounting of tapes, and maintaining computer equipment. We did not identify any significant weaknesses in the operations procedures of the computer center during our audit.

HELP DESK

The help desk function ensures that any problem experienced by the user is appropriately resolved. An effective help desk operations: 1) adequately registers all customer requests, 2) ensures that customer requests, which cannot be resolved immediately, are prioritized and assigned to appropriate personnel for resolution, and 3) ensures that procedures are in place for management to identify and monitor outstanding requests that have not been resolved in a timely manner. We did not identify any significant weaknesses in the help desk operations during our audit.

DISASTER RECOVERY

Disasters such as fire and flood can destroy a computer service center and leave its users without computer processing support. Without computer processing, many UNC Hospitals' services would grind to a halt. To reduce this risk, computer service centers develop disaster recovery plans. Disaster recovery procedures should be tested periodically to ensure the recoverability of the data center.

AUDIT FINDING 3: NO DISASTER RECOVERY PLAN

UNC Hospitals does not have a disaster recovery plan in place; however, they have received a proposal from IBM Global Services and are working with them to implement a disaster recovery plan by late summer 2002. Without a disaster recovery plan in place, the effectiveness of restoring UNC Hospital's computing services in the event of a major disaster is reduced.

Information services management should ensure that a written plan is developed containing the following:

- Guidelines on how to use the continuity plan;
- Emergency procedures to ensure the safety of all affected staff members;
- Response procedures meant to bring the business back to the state it was in before the incident or disaster;
- Recovery procedures meant to bring the business back to the state it was in before the incident or disaster;
- Procedures to safeguard and reconstruct the home site;
- Co-ordination procedures with public authorities;
- Communication procedures with stakeholders: employees, key customers, critical suppliers, stockholders and management; and
- Critical information on continuity teams, affected staff, customers, suppliers, public authorities and media.

Recommendation: Management should continue its efforts to develop and implement a disaster recovery plan for the hospital for data processing services and the user departments. Once the plan is complete and updated, it should be tested and updated at least annually or when major changes in the data processing environment are made.

Auditee's Response: ISD Management agrees with findings. The contracted services engagement will commence in 2002 with completion of plan in 2003. The objective of engagement is to address issues as stated in audit finding recommendations.

AUDIT FINDING 4: OFF-SITE STORAGE OF BACK-UP TAPES

The general ledger back-up tapes are not currently rotated to the off-site storage location and the payroll system back-up tapes are not rotated off-site on a daily basis. As a result, users may not be able to recover critical data in the event of a loss of data files. Users are not aware that they may have to recover data if the data files are not accessible from the off-site tapes.

Back-up procedures for information technology related media should include the proper storage of the data files, software and related documentation, both on-site and off-site. Back-ups should be stored securely and the storage sites periodically reviewed regarding physical access security and security of data files and other items.

Recommendation: UNC Hospitals should survey the current users to determine their requirements and needs for recovery of data files. Based on the user's requirements and needs, an appropriate backup and off-site tape rotation schedule should be established. The hospital should take the appropriate back-ups offsite on a regular basis.

Auditee's Response: ISD Management agrees with findings. Payroll (GEAC) tapes are now (as of September 2002) being rotated off-site on a daily basis. Modification to backup tape system will be complete by calendar year-end allowing for General Ledger (Lawson) back up tapes to be included in off site rotation.

[This Page Left Blank Intentionally]

DISTRIBUTION OF AUDIT REPORT

In accordance with G.S. § 147-64.5 and G.S. § 147-64.6(c)(14), copies of this report have been distributed to the public officials listed below. Additional copies are provided to other legislators, state officials, the press, and the general public upon request.

EXECUTIVE BRANCH

The Honorable Michael F. Easley	Governor of North Carolina
The Honorable Beverly M. Perdue	Lieutenant Governor of North Carolina
The Honorable Richard H. Moore	State Treasurer
The Honorable Roy A. Cooper, III	Attorney General
Mr. David T. McCoy	State Budget Officer
Mr. Robert L. Powell	State Controller
Ms. Molly Corbett Broad	President, The University of North Carolina
Mr. Eric B. Munson	President and CEO The University of North Carolina Hospitals

LEGISLATIVE BRANCH

Appointees to the Joint Legislative Commission on Governmental Operations

Senator Marc Basnight, Co-Chairman	Representative James B. Black, Co-Chairman
Senator Charlie Albertson	Representative Martha B. Alexander
Senator Frank W. Ballance, Jr.	Representative Flossie Boyd-McIntyre
Senator Charles Carter	Representative E. Nelson Cole
Senator Kever M. Clark	Representative James W. Crawford, Jr.
Senator Daniel G. Clodfelter	Representative William T. Culpepper, III
Senator Walter H. Dalton	Representative W. Pete Cunningham
Senator James Forrester	Representative Beverly M. Earle
Senator Linda Garrou	Representative Ruth M. Easterling
Senator Wilbur P. Gulley	Representative Stanley H. Fox
Senator Kay R. Hagan	Representative R. Phillip Haire
Senator David W. Hoyle	Representative Dewey L. Hill
Senator Ellie Kinnaird	Representative Mary L. Jarrell
Senator Howard N. Lee	Representative Maggie Jeffus
Senator Jeanne H. Lucas	Representative Larry T. Justus
Senator R. L. Martin	Representative Edd Nye
Senator William N. Martin	Representative Warren C. Oldham
Senator Stephen M. Metcalf	Representative William C. Owens, Jr.
Senator Fountain Odom	Representative E. David Redwine
Senator Aaron W. Plyler	Representative R. Eugene Rogers
Senator Eric M. Reeves	Representative Drew P. Saunders
Senator Dan Robinson	Representative Wilma M. Sherrill
Senator Larry Shaw	Representative Ronald L. Smith
Senator Robert G. Shaw	Representative Gregg Thompson
Senator R. C. Soles, Jr.	Representative Joe P. Tolson
Senator Ed N. Warren	Representative Russell E. Tucker
Senator David F. Weinstein	Representative Thomas E. Wright
Senator Allen H. Wellons	Representative Douglas Y. Yongue

DISTRIBUTION OF AUDIT REPORT (CONCLUDED)

Other Legislative Officials

Representative Philip A. Baddour, Jr.	Majority Leader of the N.C. House of Representatives
Senator Anthony E. Rand	Majority Leader of the N.C. Senate
Senator Patrick J. Ballantine	Minority Leader of the N.C. Senate
Representative N. Leo Daughtry	Minority Leader of the N.C. House of Representatives
Representative Joe Hackney	N.C. House Speaker Pro-Tem
Mr. James D. Johnson	Director, Fiscal Research Division

Other Officials

Chairman and Members of the Information Resource Management Commission

ORDERING INFORMATION

Copies of this report may be obtained by contacting the:

Office of the State Auditor
State of North Carolina
2 South Salisbury Street
20601 Mail Service Center
Raleigh, North Carolina 27699-0601

Internet: http://www.ncauditor.net

Telephone: 919/807-7500

Facsimile: 919/807-7647