ALAN G. HEVESI
COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

July 19, 2006

Alan D. Aviles
President & Chief Executive
New York City Health and Hospitals Corporation
125 Worth Street
New York, New York 10013

Re: Selected General Controls Over
Data Center Security
Report 2005-N-2

Dear Mr. Aviles:

Pursuant to the State Comptroller's authority as set forth in Article V, Section 1, of the State Constitution; and Article II, Section 8, of the State Finance Law, we have audited the manner in which the New York City Health and Hospitals Corporation (Corporation) protects its computer systems and data. Our audit covered the period of January 1, 2004 through August 31, 2005.

A. Background

The Corporation, the largest municipal hospital and health care system in the country, is a $4.5 billion public benefit corporation. Its mission is to extend equally to all New Yorkers, regardless of their ability to pay, comprehensive health services in an atmosphere of humane care, dignity and respect. It operates 11 acute care hospitals, 4 skilled nursing facilities, 6 large diagnostic and treatment centers, and more than 100 community health or school based clinics. These entities are grouped into seven regional semi-autonomous "networks" through which it provides medical, mental health, and substance abuse services. Its specialized services include trauma, high-risk neonatal and obstetric care, and burn care.

The Corporation's acute care hospitals serve as major teaching institutions. As the single largest provider of health care to uninsured New Yorkers, it operates a certified home health agency as well as a health maintenance organization, Metro Plus. One in every six New Yorkers receives health services at a Corporation facility. During fiscal year 2005, the Corporation had 38,183 employees and reported expenditures of $4.5 billion and revenues of $4.9 billion.

To support these operations, the Corporation maintains major computer installations. The corporate data center used to maintain business applications is run by the Corporate Information

Services unit (Information Services) in the office of the Chief Information Officer (CIO). Each network also maintains its own major data center that processes applications. In 2002, the *Journal of the American Hospital Association* listed the Corporation's North Central Bronx Hospital and Jacobi Medical Center among the 100 "most-wired" hospitals in the nation.

B. Audit Scope, Objectives and Methodology

Our audit, which covered the period January 1, 2004 through August 31, 2005, examined information technology controls over data processing. One objective of our performance audit was to determine whether the corporate office of the CIO of the Corporation has provided sufficient guidance, monitoring, and oversight to the Corporation's regional networks. The Corporation is obligated to comply with the security provisions and regulations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA); exercise strong environmental and physical controls in the Corporation's data centers; follow application control requirements that will secure the confidentiality, integrity, and availability of data; and have controls in place that will give reasonable assurance that critical data can continue to be processed after a disaster or other mishap. Another objective was to determine whether the CIO's office had established adequate business continuity and disaster recovery controls.

To accomplish our objective, we met with the CIO, Information Services and Information Systems management, the network CIOs, and application users to gain an understanding of the information technology controls established in their areas. We used auditing software to test the validity and appropriateness of user access and to look for rogue access points. We conducted observations of backup tape storage facilities; and reviewed consultant and external audit reports, policies and procedures, business continuity and disaster recovery plans, and other relevant documents.

We conducted our audit in accordance with generally accepted government auditing standards. Such standards require that we plan and perform our audit to adequately assess those operations of the Corporation that are included in our audit scope. These standards also require that we understand the internal control structure of the Corporation, and its compliance with those laws, rules and regulations that are relevant to the Corporation's operations included in our audit scope. An audit includes examining, on a test basis, the evidence supporting transactions that were recorded in the accounting and operating records, and applying other auditing procedures we consider necessary under the circumstances. An audit also includes assessing the estimates, judgments, and decisions made by management. We believe our audit provides a reasonable basis for our findings, conclusions, and recommendations.

In addition to being the State Auditor, the Comptroller performs certain other constitutionally and statutorily mandated duties as the chief fiscal officer of New York State, several of which are performed by the Division of State Services. These include operating the State's accounting system; preparing the State's financial statements; and approving State contracts, refunds, and other payments. In addition, the Comptroller appoints members to certain boards, commissions and public authorities, some of whom have minority voting rights. These duties may be considered management functions under generally accepted government auditing standards. In our opinion, these management functions do not affect our ability to conduct independent audits of program performance.

C. Results of Audit

The CIO's Office did not effectively oversee, guide, or monitor operations at regional networks. For example, the office did not formulate sufficient written policies or guidelines for acquiring and using information technology resources. Thus, Corporation employees may not be following best practices in these areas of information technology management and control. In addition, the CIO's office has not studied the cost-effectiveness of retaining the MISYS clinical record system since the mid-1990s. As a result, the Corporation lacks adequate assurances that the existing system is an optimal one from a cost benefit and a quality standpoint. Also, when we visited three network sites, we found a lack of compliance with HIPAA requirements, physical access and environmental control weaknesses, weaknesses in controls over MISYS access, concerns for the adequacy of wireless security and business continuity and disaster recovery improvement opportunities. We also noted that possibly obsolete tapes may be stored off-site unnecessarily and adequate precautions were not taken to ensure off-site tapes were recoverable.

1. Monitoring and Oversight

According to the Federal Information Systems Control Audit Manual published by the Government Accountability Office (GAO), the foundation of an entity's security control structure is security planning and management. Performed entity-wide, these efforts provide a framework and a continuing cycle of activity for assessing and managing risk, developing and implementing security policies and procedures, and assigning responsibilities. The entity's control environment sets the tone for the organization, and is a key factor in successful program planning. Relevant elements include supportive attitudes, actions, and commitment by senior management toward addressing security risks, implementation and monitoring of relevant policies, and effective communications between management and staff. More specific control techniques may be rendered ineffective unless they are supported by a strong security control environment.

In 1995, the Corporation reengineered its organizational structure to consist of regional networks, with each network comprising several hospitals and other related health facilities. The goal was to integrate long-term care, hospitals, and clinic services on a regional basis. Planning, development and management of clinical information systems was decentralized, while the central office kept control of the financial and related business systems. This decentralization led to a divergence in the way the networks and facilities adopted and customized their clinical systems, resulting in a lack of consistency and accountability.

When the Corporation examined its information technology organizational structure in 2001, it determined that decentralization was not effective. Therefore, the Corporation decided to centralize and coordinate oversight of information systems. The goal was to make the functionality in the clinical patient record system consistent throughout all of the Corporation's facilities and to consolidate its services. In the interest of consistency, responsibility for directing the Information Services and Information Systems units was assigned to the newly-created position of CIO. The networks' chief information officers were to continue working within their networks but would report to the CIO, who was to establish standards and provide strategic direction.

We found that, in response to the security requirements of HIPAA, the Information Services unit has begun developing 20 policies that are to be implemented throughout the Corporation. However, just 7 of these policies have been finalized, while 13 remain in draft form. Also, we found that Information Services has implemented 13 additional, more specific policies covering areas such as passwords, change management, security, and the acceptable uses of the Internet and e-mail. The CIO told us these policies were not based on any formal, generally accepted standards. We suggested that the CIO refer to the policies of the Citywide Information Security Architecture, Formulation, and Enforcement Unit (CISAFE) for guidance in policy development. The CIO agreed, and will utilize the CISAFE policies in developing and/or revising Corporation policies.

We visited three of the seven Corporation Networks and reviewed compliance with HIPAA information technology security provisions, physical and environmental data center controls, MISYS and logical access controls, wireless security controls and business continuity and disaster recovery controls. Our audit identified findings in each of these areas. We attribute many of our findings to inadequate oversight of Information Services and Information Systems activities.

Strong centralized oversight is also required in the development and implementation of the Corporation's clinical systems, including MISYS. Information Systems' responsibilities (headed by a Chief Medical Informatics Officer) include working with Corporation clinicians to plan and develop the existing MISYS, as well as identifying new systems that will improve the quality of patient care at the Corporation.

MISYS has served as the Corporation's clinical records system since the early 1990s. Despite this long period of usage, Information Systems has not performed any formal cost-benefit analysis to support retaining MISYS or that delineate plans for the system's future. In fact, some user management do not consider MISYS to be a modern and user-friendly system. Without a formal study of the cost benefits of retaining MISYS, Corporation management cannot be sure the highest quality and most cost-efficient clinical systems are being used. According to CIO office officials, they assumed a switch from MISYS would not be cost-effective. However, officials agree that, as part of the development of a corporate-wide strategic plan for information technology, the idea of staying with MISYS versus switching to another vendor should be subjected to a cost-benefit analysis. Such an analysis is expected to be completed by June 2006.

Many of the issues identified throughout this report stem from the absence of an adequate centralized monitoring and oversight structure. In recognition of this problem, the Corporation is now moving toward some degree of information technology standardization and consolidation. Functions that can be centralized are being consolidated, with the remainder left to the Corporation's networks. An Information Technology Executive Committee has been implemented, and meetings of the networks' chief information officers are held biweekly to discuss new systems. An Information Technology Architecture Council was expected to be in place by the end of 2005. The CIO acknowledged that improvement was needed, but asserted that significant progress has been made toward standardization and consolidation.

2. Confidential Matters

The remainder of our audit identified findings and made recommendations for corrective actions on matters pertaining to securing the Corporation's computer systems and disaster preparedness at the Corporation's data centers. These findings and recommendations were presented in detail to Corporation officials throughout the audit. To further ensure security of the Corporation's data processing operations, these findings and recommendations are not included in this report. Subsequent follow-up audits will address the detailed findings and recommendations.

Recommendations

1. *Continue efforts to strengthen the CIO's oversight and monitoring controls over the Corporation networks.*

   (Corporation officials agree and state that they have begun a project to consolidate various data centers. A one-time savings of approximately $20 million is anticipated.)

2. *Proceed with plans to prepare a formal cost-benefit analysis that will consider the alternatives of retaining MISYS or selecting another vendor.*

   (Corporation officials agree and state they have asked a consultant, Gartner, to submit a proposal for a cost benefit analysis of retaining and continuing to develop the MISYS system versus purchasing and installing a new electronic medical record system.)

3. *Implement the recommendations detailed during the audit for strengthening the computer systems security and improving disaster preparedness.*

   (Corporation officials agree and state that, along with the consolidated data centers mentioned in Recommendation 1, several of the recommendations detailed during the audit have already been implemented. They add that they will continue to implement additional recommendations.)

We provided draft copies of this report to Corporation officials for their review and formal comment. Their comments were considered in preparing this report and are included as Appendix A. Our rejoinders to the Corporation's comments are presented in Appendix B, State Comptroller's Comments.

Within 90 days after final release of this report, we request that the President of the New York City Health and Hospitals Corporation report to the State Comptroller advising what steps were taken to implement the recommendations contained herein, and where recommendations were not implemented, the reasons therefor.

Major contributors to this report were Brian Reilly, Abe Fish, Keith Dickter, Michael D'Amico and Matricia Madory.

We wish to thank the management and staff of the New York City Health and Hospitals Corporation for the courtesies extended to our auditors during this audit.

Very truly yours,

William Challice
Audit Director

NEW YORK CITY HEALTH AND HOSPITALS CORPORATION
125 Worth Street · New York · New York · 10013
212-788-3321· Fax: 212-788-0040 · E-mail: AVILESA@NYCHHC.ORG

Alan D. Aviles
President

May 12, 2006

William P. Challice
Audit Director
State of New York - Office of the State Comptroller
110 State Street
Albany, New York 12236

Re: Selected General Controls Over Data Center Security
Report 2005-N-2

Dear Mr. Challice:

Thank you for the opportunity to respond to the audit report addressing the manner in which the New York City Health and Hospitals Corporation (HHC) protects its computer systems and data.

As observed in your report and acknowledged by the Corporation's Chief Information Officer (CIO), responsibility for Information Technology Services (ITS) at HHC was not concentrated in one corporate office until the establishment of the corporate office of the CIO in 2001. Until then, management of business and financial systems was centralized while management of clinical systems and data center operations was decentralized to the seven HHC networks and monitored centrally. The corporate office of the CIO was created: (1) to provide the senior leadership of the Corporation with an overview of these disparate elements of ITS and suggest ways in which the networks could be made to work together more effectively; (2) to oversee matters of corporate concern, such as, Wide Area Network (WAN) security and Health Insurance Portability and Accountability Act (HIPAA) regulations, uniform Computerized Patient Record (CPR) functionality and, (3) to provide strategic direction to the network ITS leadership (network CIOs) ensuring corporate goals and objectives are supported by the clinical systems.

To develop and sustain the support of HHC's senior leadership for these objectives, the corporate CIO established the IT Executive Strategic Planning Committee early in 2002. The Committee, chaired by the CIO, includes the Senior Vice Presidents of the 7 regional networks, the Senior Vice Presidents for Finance, Operations, Medical and Professional Affairs and Strategic Planning and the President's Chief of Staff. The Committee meets quarterly and reviews the status of major projects, to discuss and approve/disapprove investments proposed by the CIO and/or the networks and to update the corporate ITS implementation plan and strategic direction. Examples of projects considered and approved by the Committee include, the development and installation of the Graphic User Interface front end for Misys in 2003/04; development of the Misys data warehouse 2004; the development and deployment of the Corporate Chronic Disease Registry

Appendix A

2004/05; exercising the renewal option in the Siemens contract; and, the development and installation of the e-Commerce system.

The Corporate CIO's Office has effectively carried out these responsibilities. In fact, many of the audit findings have been identified by HHC's IT staff. HHC fully understands the requirements to ensure the integrity and availability of data, especially patient-related data, and have implemented many controls to ensure:

- compliance with the security provisions and regulations of the HIPAA;
- strong environmental and physical controls in the Corporation's data centers;
- application control requirements over the Misys clinical record system;
- maintenance of secure wireless networks; and,
- maintenance of disaster preparedness controls that give reasonable assurance that critical data can continue to be processed after a disaster or other mishap.

Although we recognize some gaps in HHC's efforts to meet these responsibilities, the conclusion in your report that the CIO's Office did not effectively oversee, guide and monitor operations at the regional networks is unsupported. Some of the gaps identified were the result of limited resources and/or other priorities, not a lack of oversight. Central Office and the networks are largely in compliance with these obligations and under the direction of the CIO's Office, HHC has taken significant steps to eliminate the gaps identified long before commencement of this audit.

Comment 1

HHC is far more advanced than most health care systems in the country in the use of health care technology, particularly Computerized Physician Order Entry (CPOE) and the use of an electronic medical record (EMR). This significant distinction, that benefits our patients, was achieved without "strong centralized oversight" of the development and implementation of our Misys Computerized Patient Medical Record (CPR). We procured this system from Health Data Sciences (Misys is the current and third owner of the application), one of the few firms providing this technology in the early 1990's. Now that there are many more experienced vendors in the EMR business, it is finally possible to compare systems with respect to their quality, range of functionality, ease of use, and cost-effectiveness. In fact, in 2002, Gartner provided HHC with a study comparing the competition in the EMR marketplace, and concluded that with some additional upgrades available through Misys (which have been installed), HHC did not need to consider changing EMR systems for at least three years. Now that three years have elapsed, the office of the Corporate CIO will undertake a cost benefit analysis to evaluate a possible move away from Misys to another system.

The report cites HHC for implementing seven (7) of twenty (20) HIPAA policies. HHC began working with consultants in the winter of 2001 to develop a gap analysis (provided to the auditors during their fieldwork) and to formulate and implement policies and procedures during the early development stages of this legislation. Some policies may not have been finalized partly due to the continued evolution and clarification of the legislation. As the legislation evolved, we issued additional policies. As priorities changed, some policies remained in draft form while we adopted

the more critical ones. HHC has remained ahead of the curve on this issue, and clearly demonstrates a commitment to compliance in this area.

The statement in the report that HHC's security requirements for HIPAA policies are not based on any formal, generally accepted standards is incorrect. The policies and procedures developed for HHC by its consultants reflect Federal Regulations and standard industry practice. Moreover, as a non-mayoral agency, HHC is not bound by CISAFE requirements. However, HHC may consider CISAFE as an additional resource to supplement its current procedures.

Comment 2

The audit report claims there were three rogue (unauthorized) wireless access points – two at Lincoln, and another at Jacobi Hospital. In general, rogue access points are not a unique phenomenon, and exist in all wireless environments. It should be noted, however, that the access point at Jacobi Hospital had no connection, and created no vulnerabilities to the Network. All access points were immediately addressed and eliminated.

As a result of a Gartner ITS study completed in April 2005, HHC has taken two significant steps toward a federated governance model and the strengthening of business continuity and disaster recovery operations. We have embarked on a consolidation of our network/facility data centers into two corporate data centers to be located in the Bronx (an expansion of the existing corporate data center) and in Brooklyn on the Kings County Hospital Center (KCHC) campus. The data centers will mirror each other to provide disaster recovery/ business continuity for all systems. Should one data center fail for any reason, the other will be able to carry the full corporate load. Our goal is to have both data centers completed no later than the end of CY2007.

The feasibility study to expand the Jacobi location (which will house the corporate data center as well as the North Bronx, Queens and probably the South Manhattan Networks) is complete, and is already in the design phase. The feasibility study for the KCHC location is still in preparation however, a preferred site on the campus has been identified.

In addition, FY07 IT spending (excluding salaries and some maintenance agreements) will be consolidated in the corporate CIO's budget. This will give that office the ability to monitor and direct spending in accordance with corporate priorities.

The report alluded to a weakness over Misys and logical access - controls. We acknowledge the risks associated with full access to the patient's medical record. However, when measured against the possibility of unintentionally or mistakenly precluding a provider from obtaining all necessary information relevant to a patient's care and decision support, permitting full access is a level of risk we are willing to accept. To compensate for that risk, we will utilize the system's capability to produce audit logs to routinely monitor these reports to ensure only those authorized, within their job function, obtain access to patient records. Also, every Misys user is required to sign a corporate confidentiality agreement.

Moreover, due to the nature and structure of our networks, it would be impractical and create significant operational obstacles to continuously reassign systems access to medical professionals as they rotate within facility departments, e.g., inpatient and outpatient or among a network's facilities.

Corrective actions have been implemented for the environmental and access control issues found during the audit.

Due to HHC's size and structure, a fully centralized ITS operation is not sustainable without a sizable reallocation of finite resources, negatively impacting our primary mission of delivering patient care. The Corporate CIO's collaboration with the senior leadership and network CIOs will continue to move HHC toward a federated IT model, enabling HHC to maximize the skills and creativity available in the network IT departments. Moreover, this in turn will enable network IT departments to respond to the unique needs of their facilities, while corporate IT develops strategic direction to support business and patient care goals.

Included with this response is the Audit Implementation Plan **(Attachment 1)** which addresses all the recommendations cited in the report.

Should you have any questions concerning the content of our response, please contact Alex Scoufaras, Assistant Vice President, Internal Audits at (646)-458-5601.

Sincerely,

Alan D. Aviles

Attachment

c: F. J. Cirillo, Senior Vice President, Operations
F. Pandolfi, Corporate Chief Information Officer
W. Walsh, Senior Vice President, North Bronx Health Care Network
J. G. Leon, Senior Vice President, Central Brooklyn Health Care Network
G. Proctor, Chief Operating Officer, Central Brooklyn Health Care Network
J.R. Sanchez, Senior Vice President, Generation + /Northern Manhattan Health Care Network
D. Carr, Deputy Executive Director, North Bronx Health Care Network
A. Scoufaras, Assistant Vice President, Office of Internal Audits
M. Salamone-Greason, Chief Of Staff, Office of the President
A. Porco, Chief Information Officer, Central Brooklyn Health Care Network
M. Barremeda, Acting Chief Information Officer, Generations+/Northern Manhattan Health Care Network
C. Franklin, Deputy Chief Information Officer, North Bronx Health Care Network

MAYOR'S OFFICE OF OPERATIONS
AUDIT COORDINATION AND REVIEW
AUDIT IMPLEMENTATION PLAN

ATTACHMENT I

PART A

Audit Title: **Audit Report on Corporate Information Technology Controls over Data Processing Operations** Date: **April 19, 2006** Audit Agency: **New York State Office of the Comptroller**

Agency: **NYCHHC (OIA # 05-36)** Audit Date: **April 12, 2006** Audit No: **2005-N-2** OMB Control No: _____

RECOMMENDATION WITH WHICH THE AGENCY AGREES AND INTENDS TO IMPLEMENT	METHODS/PROCEDURES	IMPLEMENTATION TARGET DATE	PROGRAM IMPROVEMENTS/DOLLARS SAVINGS INCREASED REVENUE WITH TIME TABLE
Recommendation # 1 *To Information Services* Continue efforts to strengthen the CIO's oversight and monitoring controls over the Corporation's networks. Pg. 5	We have begun a project to consolidate our network/facility data centers into 2 corporate data centers to be located in the Bronx (at Jacobi) and Brooklyn (at Kings County). The data centers will mirror each other to provide disaster recovery and business continuity for our system. Should one data center fail for any reason, the other will be able to carry the full corporate load. In FY 2007, the IT spending (excluding salaries and some maintenance contracts) will be consolidated in the Corporate CIO's budget.	December 31, 2007 July 1, 2006	It is anticipated that there will be one time savings of approximately $20 million and several million dollars annually in operating expenses. In addition, support and maintenance of HHC's systems will be streamlined and data center operational policies and procedures standardized. The consolidated ITS budget will give the CIO's office the ability to monitor and direct spending in accordance with corporate priorities.
Recommendation # 2 *To Information Services* Proceed with plans to prepare a formal cost-benefit analysis that will consider the alternatives of retaining Misys or selecting another vendor. Pg. 5	We have asked Gartner to submit a proposal for a cost benefit analysis of retaining and continuing to develop the Misys system vs. purchasing and installing a new electronic medial record system.	Gartner's report should be completed by September, 2006.	The Corporation will have an objective basis for deciding to continue to use the Misys CPR or to procure and install a new medical record system.
Recommendation # 3 *To Information Services* Implement the recommendations detailed during the audit for strengthening the computer systems security and improving disaster preparedness. Pg. 5	See recommendation #1. In addition, several of the recommendations have already been implemented to strengthen HHC computer systems security. We will also continue to implement additional recommendations consistent with our resources and the consolidation of our data centers.	December 31, 2006	Improved security; disaster recovery/business continuity solution for all systems operational; and some operational cost savings.

State Comptroller's Comments

1. When the CIO's Office was created in 2001, it was to establish standards and provide strategic direction to the Corporation's Networks. However, at the time of our review, there was no formal, written strategic plan for the Corporation's Information Technology Services. Also, the CIO stated that decisions about infrastructure and new technology must begin to be made centrally, but that this is currently being done at lower levels. The findings in this report, as well as in the detailed confidential report, clearly show that the CIO needs to improve oversight, guidance and monitoring of the operations of the regional networks.

2. During the course of our audit, the CIO informed us that the Corporation policies were not based on any formal, generally accepted standards.

Appendix B