THOMAS P. DiNAPOLI
STATE COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

June 19, 2008

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

Re: Report 2007-F-50

Dear Mr. Aviles:

Based on the State Comptroller's authority as set forth in Article V, Section 1 of the State Constitution, and Article III, of the General Municipal Law, we have followed up on the actions taken by officials of the New York City Health and Hospitals Corporation (Corporation) to implement the recommendations contained in our audit report, *Selected General Controls Over Data Center Security*, (*2005-N-2)*.

Background, Scope and Objective

The Corporation, the largest municipal hospital and health care system in the country, is a $5.4 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. During fiscal year 2007, the Corporation had 39,371 employees and reported expenditures of $5.4 billion and revenues of $6.6 billion.

To support its operations, the Corporation maintains major computer installations. The corporate data center used to maintain business applications is run by the office of the Corporation's Chief Information Officer (CIO). Network CIO's report to the Corporation CIO, but maintain their own major data centers that process applications. The Corporation is in the process of a major data center consolidation.

Our initial audit report, which was issued on July 19, 2006, examined information technology controls over data processing. The objective of our performance audit was to determine whether the Corporation CIO provided sufficient guidance, monitoring, and oversight to the Corporation's regional networks to ensure that they comply with 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; and reasonably assure that critical data can continue to be processed after a disaster or other mishap. We determined during our audit that due to the absence of an adequate centralized monitoring and oversight structure, there was a lack of consistency and accountability for network clinical systems, no formal cost-benefit analysis to support retaining these systems and HIPAA security policies were still in draft form. Additional related findings were transmitted to the Corporation in a separate confidential report.

The objective of our follow-up was to assess the extent of implementation, as of April 17, 2008, of the three recommendations appearing in our public report, and the additional recommendations detailed in our confidential report. To further assure security of the Corporation's data processing operations, the details of the confidential recommendations and their implementation status are not included in this report. However, we discussed the detailed results of our follow-up work during the conduct of the audit.

Summary Conclusions and Status of Audit Recommendations

Overall, we found Corporation officials have made progress towards implementing the recommendations contained in the prior reports. Of the 3 public audit report recommendations, two were implemented and one was partially implemented, as detailed below. Additionally, the Corporation continues to take steps to achieve full implementation of recommendations in the confidential report.

Follow-up Observations

Recommendation 1

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

Status - Implemented

Agency Action - The Corporation revised its organizational structure such that the network CIOs report to, and the IT budget was consolidated under, the Corporate CIO. It has also initiated various committees to enhance IT governance and is working on consolidating its data centers.

Recommendation 2

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

Status - Implemented

Agency Action - The Corporation's consultant, in a December 2006 report, determined that transition to a Corporation-wide single integrated clinical solution would allow for improved continuum of care and better align with the Corporation's strategic and operational needs. The solution would also allow them to potentially avoid $78 million in investments that could off-set the estimated $150 - 290 million cost of replacement.

Recommendation 3

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

Status - Partially Implemented

Agency Action - The Corporation has made progress but has not yet fully addressed all recommendations detailed in our confidential audit report. Additional steps are needed to achieve full implementation.

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

We thank the management and staff of the Corporation for the courtesies and cooperation extended to our auditors during this process**.**

Very truly yours,

Brian Reilly
Audit Manager

cc: Alex Scoufaras, NYC HHC
Tom Lukacs, Division of the Budget