H. CARL McCALL
STATE COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

October 8, 2002

Antonia C. Novello, M.D., M.P.H., Dr. P.H.
Commissioner
Department of Health
Corning Tower, Empire State Plaza
Albany, NY 12237

Re: Report 2002-F-17

Dear Dr. Novello:

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 reviewed the actions taken by officials of the Department of Health (Department) as of September 9, 2002, to implement the recommendations contained in our audit report, *General and Application Controls Over the Health Information Network* (Report 2001-S-4). Our report, which was issued on August 15, 2001, reviewed selected aspects of the general and application controls in place over the Health Information Network (Network) for the period April 1, 1999 through April 13, 2001. Our primary objective was to determine whether the system of controls in place over the Network was sufficient to prevent unauthorized users from accessing confidential information.

Background

In 1998, the Department developed the Network as part of a cooperative agreement with the United States Center for Disease Control to provide the rapid electronic interchange of information between health officials at State and county health departments essential for the rapid detection, response, and abatement of disease outbreaks. The information exchanged ranges from hospital statistics, birth and death statistics, and communicable disease alerts to confidential health information about individuals.

The Network is a web-based system that users access through dedicated lines, shared lines, or the Internet. The Network consists of central servers, databases, applications, and other network infrastructure. The mission of the Network is to provide for the timely, accurate, appropriate, and secure exchange of health information among users at the Department, the 57 county health departments throughout the State, and the New York City Department of Health. As of September 9, 2002, there were approximately 2,960 Network users.

The Department's information technology unit, the Information Systems and Health Statistics

Group (ISHSG), is responsible for Network operation. Within ISHSG, the Bureau of Healthcom Network Systems Management develops and maintains the Network, and the Production Control Unit (PCU) monitors Network usage. The Department's Health Communications Services Bureau is responsible for Network security.

Summary Conclusions

In our prior audit, we found that the controls for preventing unauthorized access to the Network were generally adequate, but improvements could be made in certain controls to provide even better protection. We also found that plans needed to be developed and other actions taken to prevent service interruptions and a loss of information from power failures, natural disasters, and other such events.

In our follow-up review, we found that Department officials have made progress in implementing the recommendations contained in our prior audit.

Summary of Status of Prior Audit Recommendations

Of the four prior audit recommendations, Department officials have implemented two recommendations and partially implemented two recommendations.

Follow-up Observations

Recommendation 1

Take steps to enhance controls over access to the Network. At a minimum this should include:

- *formally reviewing application logs;*
- *reinforcing the requirement to provide immediate notification of users whose accounts should be disabled;*
- *monitoring and disabling inactive accounts, including but not limited to exploring the feasibility of shortening the time frame for monitoring user access rights at the county level;*
- *requiring passwords to automatically expire for individuals who have temporary access;*
- *shortening the time period when the Network automatically logs a user off after a period of inactivity;*
- *decreasing the number of failed login attempts before a user's account is investigated and disabled; and*
- *ensuring that all county health departments are connected to the Network via firewalls.*

Status – Partially Implemented

Agency Action – The Department has made significant progress in implementing this recommendation. Department officials have complied fully with six of the seven control elements and are currently working on the remaining control element. The Department has developed an application program that scans all user access codes and compares data from a valid user file in a search for unauthorized or inactive codes. The "Zero Report" helps identify unauthorized attempts to access Network applications. However, officials stated that, although the application program is available for all program areas to use, just a few have taken advantage of it. As a result, this part of the recommendation has been only partially implemented.

In addition to the application program, Department regulations require immediate notification of users whose accounts should be disabled because of a change in employment status or job duties. Officials told us that, since our prior audit, the Department has appointed unit staff as Computer Security Coordinators who are responsible for notifying the Production Control Unit immediately when an employee's employment status changes, such as the assumption of a new job title or duties, retirement, etc. However, these new procedures pertain only to Department program areas. To help ensure that county departments provide timely notification of accounts that should be disabled, the Department sent letters to the county Commissioners informing them of the importance of proper and timely notification. In addition, the Department has added the notification requirement to each county's "Public Health Preparedness & Response Plan." If a county does not verify the list and notify the Department of changes, it can lose funding.

The Department has also implemented new procedures for monitoring and disabling inactive accounts. According to officials, the Department has put in place a program to scan all user accounts for accounts that have not been used within the last five months. This process is automatic and runs continuously.

During our prior audit, we identified several features available to Network users that should be changed to provide better access control. We found, for example, that the access for staff with temporary accounts was not cancelled automatically when the temporary assignment was completed. We also found that the period for which users could remain inactive before being logged off was too long in comparison to Industry standards, and that the number of times a user could attempt a login without being investigated needed to be reduced to restrict the possibility of unauthorized use of the Network. Our follow-up review found that the Department has taken steps to improve access controls by automatically eliminating temporary accounts, reducing the session timer, and reducing the number of login attempts before the user is logged out of the Network.

Lastly, our prior audit had found that some county departments were connecting to the Network without going through the firewall. Department officials stated that all counties are now behind a firewall. To ensure that county departments connect to the Network using the proper connection procedures, the Department controls all access lines and can direct all

calls through the firewall. Officials also told us they developed firewall rules that were provided to all counties.

Recommendation 2

Take the steps necessary to install an Uninterruptible Power Supply system.

Status – Implemented

Agency Action – In November 2001, the Department received and installed an Uninterruptible Power Supply system.

Recommendation 3

Develop a formal written disaster contingency plan that includes a comprehensive disaster recovery procedure.

Status – Partially Implemented

Agency Action – The Department has applied to the Office of General Services (OGS) for a location outside the Department's main offices that could serve as a disaster contingency and recovery site. OGS officials have tentatively selected a site and have told the Department it would be ready around the first or second quarter of 2003. The Department has also hired an outside consultant to assess its disaster contingency and recovery needs. This was expected to be completed by Fall 2002. Officials tell us, however, no formal written contingency disaster plan has been prepared, except for the consultant's assessment.

Recommendation 4

Conduct periodic reviews of the accuracy of the data entered onto the Network by Vital Records Department employees.

Status – Implemented

Agency Action – Department officials told us that they perform several types of analysis on data and produce different types of data error reports. For example, one, a frequency error report, identifies incorrect or inconsistent numbers. Another report generates logic or code ranges and makes comparisons between fields. Staff review the reports and compile exception lists, which help them determine why or how the error was created. To collect hospital statistics, the Department contracted to survey selected hospital data and compare the hospital data with actual records. These results have enabled the Department to assess the reliability of the hospital data that Department staff was receiving.

Major contributors to this report were John Buyce, Larry Wagner, and Don Wilson.

We would appreciate your response to this report within 30 days, indicating any actions planned or taken to address any unresolved issues discussed in this report. We also thank the Department management and staff for the courtesies and cooperation extended to our auditor during this review.

Very truly yours

Frank J. Houston
Audit Director

cc: Thomas Howe
Deirdre A. Taylor