H. CARL MCCALL
STATE COMPTROLLER

A.E. SMITH STATE OFFICE BUILDING
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

August 15, 2001

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

Re: General and Application Controls Over the Health Information Network
Report 2001-S-4

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 audited the general and application controls over the Health Information Network (Network) at the Department of Health (Department). Our audit covered the period April 1, 1999 through April 13, 2001.

A. Background

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

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 April 13, 2001, 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 monitors Network usage. The Department's Health Communications Services Bureau is responsible for Network security.

B. Audit Scope, Objective and Methodology

We audited selected aspects of the general and application controls in place over the Network for the period April 1, 1999 through April 13, 2001. The primary objective of our performance audit was to determine whether the system of controls in place over the Network is sufficient to prevent unauthorized users from accessing confidential information. To accomplish our objective, we interviewed staff from the Department and from four county health departments (Oneida, Onondaga, New York City and Westchester), and we reviewed Department policies and procedures. To assess the level of compliance with Department policies and procedures, we performed audit tests at the above county health departments, which were selected judgmentally based on the number of users. We also performed the same audit tests of two Department programs: the communicable disease program within the Division of Epidemiology and the Vital Records program within the Bureau of Production Systems Management. The scope of this audit did not include a vulnerability assessment of the Network through the use of a commercial vulnerability assessment product, such as Internet Security Scanner, nor did we test security by attempting to hack in and infiltrate the Network.

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 Department operations that are within our audit scope. Further, these standards require that we understand the Department's internal control structure and compliance with those laws, rules and regulations that are relevant to the operations included in our audit scope. An audit includes examining, on a test basis, evidence supporting transactions recorded in the accounting and operating records, and applying such other auditing procedures as we considered necessary in 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.

We use a risk-based approach when selecting activities to be audited. We therefore focus our audit efforts on those activities we have identified through a preliminary survey as having the greatest probability for needing improvement. Consequently, by design, we use our finite audit resources to identify where and how improvements can be made. Thus, we devote little effort to reviewing operations that may be relatively efficient or effective. As a result, we prepare our audit reports on an "exception basis." This report, therefore, highlights those areas needing improvement and does not address activities that may be functioning properly.

C. Results of the Audit

We found that the general and application controls over the Network are generally adequate to provide reasonable assurance against unauthorized access. The Department has taken steps in

accordance with government standards that require that sensitive and confidential data be transmitted in a secure manner to and from authorized users. However, we found that certain controls can be strengthened to further ensure that access to the Network is appropriate, that Network information recovery and disaster preparedness is adequate, and that information uploaded to the Network from hardcopy sources is accurate. Department officials are aware of these deficiencies and have taken steps to address many of them.

1. Access Controls

a. Review of Application Logs

To detect and prevent unauthorized access to Network information, management should establish a formal review process of the application logs to identify unauthorized attempts to access Network applications. However, the Department has not established such a formal review process. Instead, the Department leaves it up to individual Department programs to determine whether to review these logs. We determined that the communicable disease program within the Division of Epidemiology reviews these logs. However, Vital Records does not monitor unauthorized access attempts to Network applications used by the Vital Records office. Department officials stated that an unauthorized user could not hack into an application by repetitively trying to access it; if this occurs, the URL will continue to produce a form to request access to the application. However, Department officials acknowledge that it is important to have a formal review of the log. Officials told us that technical staff are developing automated processes to scan the Network application logs for anomalies and usage patterns. This information will be used to provide reports to Department managers to assist them in monitoring usage of their applications.

b. Disabling Accounts of Users Who No Longer Require Network Access

Controls over access include regularly checking users' authorization, verifying their continuing need for access and monitoring the activity levels in user accounts. The Department recognizes the importance of limiting Network access to authorized individuals, and has developed several policies and procedures intended to ensure that only individuals whose jobs require it have such access. According to Department procedures, individual Department units and county health departments are required to immediately notify the Production Control Unit (PCU) when an employee with Network access has left employment, or when the employee no longer needs access because of a change in job duties. Since these individuals no longer require access to the Network, their accounts should be disabled. To help identify unauthorized users, the PCU monitors monthly reports from the Department's human resource office that identify persons who have left State employment. In addition, the PCU sends each county health department a list of authorized users on a cyclical basis, and requests that county officials review the list to identify persons who do not require access to the Network.

However, PCU officials informed us that Department units and county health departments generally do not notify them promptly when employees leave or no longer need access, as required by Department procedures. Officials further indicated that county health departments do not always review the lists and return them to the PCU in a timely manner. We also found that the Department

does not actively investigate user accounts that have not shown activity for a certain period of time, and does not automatically disable temporary accounts after a specific time. Therefore, there is increased risk that unauthorized Network users could have active accounts for extended periods of time.

We conducted audit tests to determine the number of users who have unnecessary access to the Network, and the length of time they held such access. For the period January 1, 2000 through February 20, 2001, we found that some county health department and Department users who no longer required access to the Network had not had their Network accounts disabled in a timely manner. For the county health departments and Department program areas we visited, officials reported that 42 users no longer needed access to the Network during this period because of a change in employment status or a change in job duties. From the Department data we reviewed, we determined the following: 4 accounts were disabled before the users terminated their employment; 7 accounts were disabled within one month of termination; 8 accounts were disabled within one to two months of termination; 12 were disabled within three months to one year of termination; and 1 account was not disabled until 643 days after termination. The Department had not yet disabled the remaining ten accounts. At the time of our test, these 10 accounts had remained active from between 19 and 385 days.

We also identified instances in which employees had access to the Network, but did not need it to carry out their job duties. We determined that 9 of 50 judgmentally selected users (18 percent) at the Department programs and county health departments we visited did not need access to the Network, but still had active accounts. At the county health departments, 4 of 29 users did not need access; at the Department, 5 out of 21 users had unnecessary access.

Given the risk involved in allowing inappropriate or unnecessary access to confidential Network data, the Department should take a number of steps to strengthen access controls. First, we believe the PCU should send county health departments lists of authorized users more frequently than the current cycle. Second, we encourage the Department to inform county health officials that they can review user access rights in their county directly on the Network. Westchester Health Department officials told us they were not aware of this Network application. Finally, it is also essential that the Department monitor user account activity and set a specific time period after which temporary accounts expire.

In response to our preliminary findings, Department officials stated that since county health departments are very busy, and relatively slow in completing reviews of user lists, the current interval is the only practical one for this control procedure. Officials also pointed out that the PCU calls county health departments as a follow-up measure to help compensate for their lengthy response times. Nevertheless, the Department should explore the feasibility of reducing the current interval because it is too long a period to allow potentially unauthorized users to have access to the Network. In addition, Department officials indicated that they plan to promote the availability of reviewing user access rights at the county level. Further, Department officials stated that technical staff are researching usage patterns of Network accounts and will work with Department units and the New York State Association of County Health Officials to develop a process for timely certification of

Network accounts, especially inactive accounts, that will be effective and workable within their daily business routines.

c. Inactive Personal Computers

The Network is set to log users out after several hours of inactivity. Due to the sensitive and confidential nature of Network information, we believe that the current interval is too long a period of time for Network PCs to remain logged on. Consequently, the likelihood of an unauthorized user accessing an idle PC that is logged onto the Network is greater. We found that some users have taken it upon themselves to decrease the log out times at their individual workstations. For instance, a nurse at one county health department had her computer station set to automatically log out after one minute of inactivity. Department officials indicate that they will be researching the usage patterns and shorten the session timer as appropriate.

d. Failed Login Attempts

According to industry guidelines, several invalid password attempts should result in disabling an account or ID. More specifically, three invalid passwords in four hours should lock an account. During our audit, we found that Network settings exceeded industry guidelines before an account is investigated or disabled. In response to our preliminary findings, Department officials stated that they have decreased the number of tries before lockout to determine user impact, and that further downward adjustments will be made, as appropriate.

e. Firewalls

We found that not all county health departments connect to the Network through a firewall. Some county health departments still connect via a filtering router, which is similar to a firewall, but is less secure. According to Department officials, they have not had time to implement the use of firewalls for all county health departments because the Network is relatively new. Officials indicated that all county health departments would be migrated to the firewall environment in the near future.

2. Recovery Controls

The Department should have an Uninterruptible Power Supply (UPS) system in place to ensure it can keep the Network up and running in the event of an extended power failure. In addition, the Department should have a formal written business continuance and disaster recovery plan to provide adequate assurance it can survive any type of disaster. However, we found the Department has not developed a UPS or a formal disaster contingency plan. Without proper preparedness, Department operations, including Network functions, could be jeopardized in the event of a disaster. Department officials indicated that the lack of a UPS and disaster recovery plan is due to funding constraints. They stated they are in the process of purchasing a UPS for the Network, but that no specific portion of the Department's budget is dedicated to developing a formal written disaster contingency plan that includes a comprehensive disaster recovery procedure.

3. Quality Controls

Employees in Vital Records upload hardcopy data they receive from localities to the Network. However, there is no control procedure in place to verify that employees enter this data correctly. Without a control procedure, such as periodic reviews to confirm the accuracy of data entered by Vital Records staff, the Department does not have adequate assurance that such Network data is reliable.

Recommendations

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.*

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

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

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

We provided draft copies of this report to Department officials for their review and comment. We considered the Department's comments in preparing this report and included them as Appendix A. Department officials generally agree with our recommendations and indicated the steps they have taken or will take to implement them.

Within 90 days after the final release of this report, as required by Section 170 of the Executive Law, the Commissioner of the New York State Department of Health shall report to the Governor, the State Comptroller and the leaders of the Legislature and fiscal committees, 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 Howard Feigenbaum, Ed Durocher, Andrea Inman, Brian Krawiecki, Tim Marten and Sri Ramen.

We wish to thank the management and staff of the Department for the courtesies and cooperation extended to our auditors during the audit.

Very truly yours,

Kevin M. McClune
Audit Director

cc: Deirdre A. Taylor

STATE OF NEW YORK
DEPARTMENT OF HEALTH
Corning Tower The Governor Nelson A. Rockefeller Empire State Plaza Albany, New York 12237

Antonia C. Novello, M.D., M.P.H., Dr.P.H.
Commissioner

Dennis P. Whalen
Executive Deputy Commissioner

August 6, 2001

Kevin M. McClune
Audit Director
Office of the State Comptroller
Alfred E. Smith State Office Building
Albany, New York 12236

Dear Mr. McClune:

Enclosed are the Department of Health's revised comments on the Office of the State Comptroller's revised draft audit report 2001-S-4, entitled "Health Information Network".

Thank you for the opportunity to comment.

Sincerely,

Dennis P. Whalen
Executive Deputy Commissioner

Enclosure

Appendix A

Department of Health
Revised Comments on the
Office of the State Comptroller's
Revised Draft Audit Report
2001-S-4 Entitled
"Health Information Network"

The following are the Department of Health's (DOH) revised comments in response to the Office of the State Comptroller's (OSC) Revised Draft Audit Report 2001-S-4 entitled "Health Information Network".

The Health Information Network (HIN) provides timely access to information critical to the practice of public health at the local level. Officials at the United States Center for Disease Control and Prevention (CDC) often cite New York as one of the leading states in health information infrastructure and the HIN as a model for integrated public health networks. The Department is mindful, as well, of its responsibilities to safeguard the information found on the HIN. It fully adheres to the access standards required by the CDC and New York State law. The Department believes its access and security protocols are among the most rigorous in the nation and meets the highest, appropriate industry standards.

The HIN-web supports the exchange of a wide variety of health related information including:

- electronic disease surveillance;
- posting health alerts;
- blood level surveillance;
- electronic birth data;
- statistical data queries; and
- general health program information.

The HIN provides both the Department and local health districts with the ability to obtain real time information on public health outbreaks such as West Nile Virus, thereby providing public health officials with as much fact based information as possible to make informed public health decisions.

The following are the Department's responses to OSC's specific recommendations.

Recommendation #1:

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

a. formally reviewing application logs; reinforcing the requirement to provide immediate notification of users whose accounts should be disabled;

Recommendation #1 (cont'd):

b. 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;

c. requiring passwords to automatically expire for individuals who have temporary access;

d. shortening the time period when the Network automatically logs a user off after a period of inactivity;

e. decreasing the number of failed login attempts before a user's account is investigated and disabled; and

f. ensuring that all county health departments are connected to the Network via firewalls.

Response #1:

a. Staff are developing and testing utilities that allow program areas to monitor usage and access to their HIN applications from the logs. Usage of the monitoring application by program areas will itself be formally monitored by Production Control Unit (PCU) staff to ascertain whether program areas are monitoring usage of their applications. The implementation time line is the second quarter of 2001.

b. Staff are working on a process to improve the timeliness of notification to the PCU of Department users who have left the agency or whose accounts should be disabled. A HIN application which allows local county HIN coordinators to review access and application permissions is available for usage by HIN-coordinators. A letter explaining its importance has been sent, along with training materials on its use, to all county health departments. The PCU will use the application usage monitor described above to formally review and monitor usage of this application by HIN coordinators to assure that local users are being actively reviewed by the coordinators. Staff will be working with New York State Association of County Health Officials (NYSACHO) to promote usage of the monitoring application and timely response to the HIN user re-certification letter. Also, all inactive HIN accounts have been and will be disabled in the future. Staff are evaluating the impact and will shorten the duration accordingly.

HIN access granting procedures require DOH management or county health commissioners to confirm, in writing, that access is appropriate to their users requesting access. As the request is made and signed by a commissioner/coordinator and as the security agreement includes language asserting that usage must be necessary to carry out ones job, it is understood that the commissioner believes staff access is necessary and appropriate for their job. Valid uses of the HIN include users who would be expected to use the system infrequently, such as in a health emergency.

Response #1 (cont'd):

In these circumstances initiating a request/signoff and validation process *de novo* in order to access the HIN

for critical information may not be conducive to a rapid response by first responders at the local level, especially during off-hours.

c. This capability is available. Staff are working on making it available to PCU and to train them in its use.

d. Staff have decreased the automatic timing out and are monitoring the impact on HIN workflow and will adjust this downward as appropriate. Staff are investigating additional capabilities for decreasing timing on session inactivity without interfering with workflow processes of local health departments.

e. Staff have decreased the number of consecutive failed attempts and are continuing to monitor impact on HIN workflow to ascertain the impact of decreasing it further.

f. At the time the audit started, the Department had been actively engaged in converting the few remaining counties to access HIN web through the firewall

Recommendation #2:

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

Response #2:

A UPS has been ordered and delivery is expected soon. Installation is anticipated to be completed by October 2001.

Recommendation #3:

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

Response #3:

A draft proposal for a disaster recovery capability has been developed. The plan will be forwarded to OGS and will need the approval of OGS' space planning unit.

Recommendation #4:

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

Response #4:

The data provided to local health units through the HIN must be provided as quickly as possible so the units can use the data to make contact with high risk mothers and infants, who may need care. The data abstracts provided are made available as soon as the data are received, usually the same day. Data are edited for quality and the files are changed to reflect measures taken. This process takes 60 to 90 days to complete.

These data are available to health units for analysis on the HIN. Local health units can also request data for analyses.

Periodic surveys are also conducted to assess data quality. The results of these surveys are used to inform data submitters of ways to improve data quality. The results of a survey conducted using 1999 births should be ready by Fall 2001. The results will be shared with hospitals that submit data.