Audit of Health Department - Public Health Laboratory - AIX and SoftLab System Controls

MARTIN MATSON
City Comptroller

AYCHA SIRVANCI, CPA
Audit Manager
City of Milwaukee, Wisconsin

March 2014

Table of Contents

Martin Matson
Comptroller

John M. Egan, CPA
Deputy Comptroller

Glenn Steinbrecher, CPA
Special Deputy Comptroller

Toni Biscobing
Special Deputy Comptroller

Office of the Comptroller

March 25, 2014

Honorable Tom Barrett, Mayor
The Members of the Common Council
City of Milwaukee

Dear Mayor Barrett and Council Members:

The attached report summarizes the results of our audit of the Health Department - Public Health Laboratory ("the Laboratory") - AIX and SoftLab System Controls. The objectives of the audit were the following: determine whether the access controls over the AIX and SoftLab systems are in compliance with City Password Policy and best-practice configuration; determine whether the Laboratory is in compliance with the Health Insurance Portability and Accountability Act (HIPAA); assess the adequacy of the Information Technology (IT) Governance process over the Laboratory information system; and assess whether the controls over the server tape backups are adequate to properly safeguard the system.

Overall, the audit concluded that the internal controls in place over the AIX and SoftLab System are adequately designed and operating effectively. However, for certain controls, identified within this report, gaps exist in the control design or operational effectiveness that exposes the Laboratory to risks. This report identifies nine recommendations to address these issues.

Audit findings are discussed in the Audit Conclusions and Recommendations section of this report, which is followed by management's response.

Appreciation is expressed for the cooperation extended to the auditors by the staff of the Health Department.

Sincerely,

Aycha Sirvanci

Aycha Sirvanci, CPA
Audit Manager

AS:gjl

City Hall, Room 404, 200 E. Wells Street, Milwaukee, WI 53202 • Phone (414) 286-3321 • Fax (414) 286-3281
www.milwaukee.gov/comptroller

I. Audit Scope and Objectives

The scope of the audit includes the access and application controls over the AIX and LIS systems administered by the City of Milwaukee ("the City") Public Health Laboratory ("the Laboratory"). The audit focused on whether the access and application control over the AIX and LIS systems were in compliance with best-practice configuration and adequate to properly safeguard personal health information, while also complying with regulatory security standards. The audit also focused on the adequacy of the overall IT Governance process over the management of the Laboratory's information system.

The City is considered a covered entity and legally required to comply with the the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its regulations, the Privacy Rule and the Security Rule. The regulations protect the privacy of an individual's health information and govern the way certain healthcare providers and benefits plans collect, maintain, use, and disclose protected health information ("PHI"). The audit covers the Laboratory's activities for calendar year 2013. The audit does not include daily laboratory-processing operations, which include receiving specimens, recording, and testing, with the exception of the controls over how the release of PHI test results occur. The audit does not include testing cash controls over Laboratory test-fee revenue.

The audit's methodology included developing an understanding of processes and controls for the AIX operating system, SoftLab and SoftMic applications, and the security measures surrounding the database containing protected health information. The audit procedures were developed to evaluate the processes and controls, to meet the audit's objectives that included process walk-throughs, inspection of relevant control documentation, system-flowchart analysis, security-configuration reviews, and detail tests of controls. Specific procedures and tests were conducted that:

- Assessed whether the Laboratory complied with the City Password Policy and applicable HIPAA regulations;
- Compared the Laboratory's AIX configuration against the IBM-recommended configuration and best-practice criteria;

- Tested a sample of confidentiality agreements for employees' signatures and whether the agreement was signed within 30 days of employment;
- Tested backup procedures for proper periodic tape backup and vault storage of the tapes; and
- Assessed the adequacy of the IT Governance process over the Laboratory's information system.

Audit procedures were executed during November and December 2013. Internal Audit believes that the evidence obtained provides a reasonable basis for the audit's findings and conclusions, based on the audit's objectives.

The objectives of the audit were to:

- Determine whether the access controls over the AIX and SoftLab systems are in compliance with City Password Policy and best-practice configuration;
- Determine whether the Laboratory is in compliance with HIPAA regulation;
- Assess the adequacy of the IT Governance process over the Laboratory's information system; and
- Assess whether the controls over the server-tape backups are adequate to properly safeguard the system.

II. Organization and Fiscal Impact

The mission of the Milwaukee Health Department is to ensure that services are available to enhance the health of individuals and families, promote healthy neighborhoods, and safeguard the health of the Milwaukee community. The city of Milwaukee Health Department is a leader in assuring that Milwaukee is the healthiest city in the nation, with the best personal health care, environmental health, and population-based preventive services possible.

The Laboratory's mission is to assist the Health Department in guarding the public's health by providing quality laboratory services for monitoring acute and chronic diseases and the environment through assessment, surveillance, epidemiology, and dissemination of information.

The Laboratory's vision is to continue providing quality service, to both internal and external clients of the Laboratory, in response to dynamic epidemiological variables, as well as to be responsive to the healthcare community's changing demands.

The Laboratory is a division of the Milwaukee Health Department, comprised of multiple laboratories, all of which utilize special technologies to help health professionals analyze the risk of disease, prevent infectious exposures, and diagnose illness. The microbiology laboratory tests for bacteria and parasites that cause disease, including tuberculosis, sexually transmitted infections, contaminants of food and water (both potable and swimming). The chemistry laboratory analyzes environmental toxins, including lead in children's blood and in dust, paint and soil, as well as food contaminants, environmental pollutants, and industrial hazards. The virology laboratory tests for viruses that cause AIDS, influenza, diarrhea, meningitis, and other diseases in both environmental and clinical samples.

The Laboratory processes over 80,000 specimens per year with over 500,000 results accumulated in the database. Its fee-for-service tests generate approximately $200,000 in revenue for the City each year. While providing diagnostic and surveillance capabilities for communicable and emerging infectious diseases, including STDs, the Laboratory also supports emergency bioterrorism preparedness and national-level responses, as well as environmental health, such as lead poisoning and water and food safety efforts.[1]

The Laboratory uses IBM's AIX version 6.1 as its operating system to support applications. SoftSec is the security module that enables the administrator to authorize access to SoftLab/SoftMic. The SoftLab/SoftMic systems have approximately 56 end users, all of whom are City employees, except for two authorized State health users. The only other system access is the Administrator and IT personnel from software vendor SCC Soft Computer. One City Laboratory Administrator grants user access to SoftLab; and only this Administrator has access to AIX. AIX and SoftLab are both run on a City-owned server, located in a high-security area in a City owned facility. The operating system, application software and database are all housed in one machine.

[1] *City of Milwaukee 2013 Adopted Plan and Budget Summary*

III. Audit Conclusions and Recommendations

The Laboratory information system should provide three very important qualities of data confidentiality, data integrity, and data availability. Data confidentiality means that appropriate controls should be in place to authorize and authenticate users, based on job responsibilities and the least-privilege access principle. Data integrity involves the accuracy of the system's reported results. Data availability involves the ability to access data easily, where and when needed and, most importantly, to minimize or eliminate system downtime and business disruption events that can lead to lost productivity and service interruptions to citizens.

Overall, the audit concluded that the internal controls in place over the AIX and SoftLab System are adequately designed and operating effectively. However, for certain controls, cited within this report, there are gaps in the control design or operational effectiveness that expose the Laboratory to risks. The access controls over the AIX and SoftLab systems are in compliance with City Password Policy, except for password length and alphanumeric requirements. The Laboratory is in compliance with the HIPAA regulations, except for not designating a Security Official, an outdated risk analysis and no formal quality review process. The IT Governance process over the Laboratory's information system is adequate, except for three low risk configuration items and contingency planning. There were no exceptions noted regarding the server-tape backup process; the controls over the server-tape backups are adequate to properly safeguard the system. This report specifies the following nine recommendations to address these issues:

1. Identify and designate a Security Official.
2. Perform a HIPAA-compliant risk analysis documenting the process and results.
3. Develop and implement a formalized quality-review process.
4. Configure all passwords to comply with the City's Password Policy.
5. Perform user-access reviews twice per year including the approval of the Laboratory Director.
6. Configure the software to the manufacturer's recommended settings.
7. Designate and train a Backup System Administrator.

8. Implement procedures for periodic testing and revision of contingency plan.
9. Upgrade the water-based fire sprinkler above the server to a chemical-based fire-suppression system.

Additional details regarding the recommendations for improvement are provided in the remaining sections of this report.

A. Compliance with HIPAA

The Laboratory is considered a HIPAA-covered entity and legally required to comply with HIPAA and its regulatory standards, the "Privacy Rule" and the "Security Rule", because it directly handles PHI or Personal Health Records (PHR). The law protects the privacy of an individual's health information and governs the way certain healthcare providers and benefits plans collect, maintain, use, and disclose PHI. PHI refers to demographic information, medical history, test and laboratory results, insurance information, and other data that is collected by a healthcare professional in order to identify an individual and determine appropriate care. The patient or legal guardian is the only individual with the capacity to authorize the release of PHI.

The audit included procedures to determine the Laboratory's compliance with the specific provisions of HIPAA. Specifically, Laboratory activities that are governed by HIPAA's rule "Security Standards for the Protection of Electronic Protected Health Information," found at 45 CFR Part 160 and Part 164, Subparts A and C, commonly referred to as the "Security Rule". The Security Rule was adopted to execute HIPAA provisions.

For certain HIPAA compliance controls, cited within this report, there are gaps in the control design or operational effectiveness that expose the Laboratory to the risks identified in the audit.

Security Official

The second standard of HIPAA's Administrative Safeguards section is entitled "Assigned Security Responsibility." The standard outlined in §164.308(a) (2) requires that covered entities:

- *"Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart [the Security Rule] for the entity."*

The purpose of this standard is to identify who will be operationally responsible for assuring that the covered entity complies with the Security Rule. Covered entities should be aware of the ability to delegate responsibilities when assigning security duties. While one individual must be designated as having overall responsibility, other individuals in the covered entity may be assigned specific security responsibilities (e.g., facility security or network security). The Laboratory does not have a designated Security Official, as required under HIPAA regulations. The former designated Security Official left City employment.

Recommendation 1: Identify and designate a Security Official.
This individual will be operationally responsible for assuring that the covered entity complies with HIPAA's Security Rule, including the configuration of system security.

HIPAA Compliant Risk Analysis

A risk analysis is required by section *§ 164.308(a) (1) (ii) (A).* The specification of the risk analysis's implementation requires covered entities to:

- *"Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity."*

The Security Rule's Administrative Safeguard's require covered entities to perform risk analysis as part of their security-management processes. The risk analysis and management provisions of the Security Rule are addressed separately to determine which security measures are reasonable and appropriate for a particular covered entity, risk analysis affects the implementation of all of the safeguards contained in the Security Rule.[2]

[2] *Department of Health and Human Services – HIPAA Security Series 2009*

The last HIPAA-compliant risk analysis was performed approximately seven (7) years ago. During this period, the Laboratory experienced a significant number of priorities, as well as staff reductions, and staff turnover.

Recommendation 2: Perform a HIPAA-compliant risk analysis documenting the process and results.

The risk analysis process includes, but is not limited to, the following activities:

- Evaluate the likelihood and impact of potential risks to PHI;
- Implement appropriate security measures to address the risks identified in the risk analysis;
- Document the chosen security measures and, where required, the rationale for adopting those measures; and
- Maintain continuous, reasonable, and appropriate security protections.

Risk analysis should be an ongoing process, in which a covered entity regularly reviews its records to track access to PHI and detect security incidents, periodically evaluates the effectiveness of security measures put in place, and regularly reevaluates potential risks to PHI. One significant benefit to performing the risk analysis is to assist the Laboratory in directing its own limited resources to the areas identified with the highest residual risk. This activity synchronizes well with the periodic quality review performed by the Compliance Official.

Formalized Quality-Review Process

Covered entities must implement ongoing monitoring and evaluation plans. Covered entities must periodically evaluate their strategy and systems to ensure that the security requirements continue to meet their organizations' operating environments. The standard is outlined in §164.308(a) (2):

- *"Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations changes affecting the security of electronic protected health information, which establishes the extent to which an entity's security policies and procedures meet the requirements of this subpart [the Security Rule]."164.*

The Laboratory has no formalized quality-review process in place to monitor and evaluate HIPAA compliance, as required by law.

Recommendation 3: Develop and implement a formalized quality-review process.
The process should monitor and evaluate HIPAA-regulatory compliance. The results of the process should be utilized to better focus limited staff resources on mitigating the Laboratory's residual risks identified during the risk assessment. The process should be performed at all Laboratory clinic and service sites. Identified errors should be remedied and the results of the review should be tracked, documented, and reported to the Laboratory Director on a periodic basis. Additionally, the information gathered from the quality-review process could provide valuable input to the ongoing HIPAA-compliant risk analysis and provide focus for future quality reviews by identifying trends and training opportunities.

B. Compliance with the City Password Policy

All City departments that have information systems and networks need to ensure that access to these systems is restricted, to safeguard the City's assets and data. Passwords are an important aspect of computer-system security. Passwords help protect the integrity of the City's data and safeguard the City's assets and data against fraud, misuse, and theft. Employees with administrative and regular access to Active Directories and City applications are responsible for taking the appropriate steps to select and secure strong passwords efforts.[3]

City information systems and networks are required to enforce strong passwords that meet the minimum-security standards outlined in the City's policy. Password strength should reflect the environment that the information system is deployed in and the likely threats it will face. However, minimal password requirements, as outlined in the policy, are required to provide baseline protection of the City's data and information systems. Information Systems administrative personnel charged with the management of Active Directories and applications

[3] *City of Milwaukee Password Policy dated June 11, 2011*

should configure the end-user passwords to enforce strong password requirements as outlined. Administrative accounts, such as the Domain Administrator, Application Administrator, and Database Administrator, must also comply with the strong password requirements, as outlined in the policy.

SoftLab Password Configuration

Currently, the SoftLab password configuration does not comply with the City's Password Policy. SoftLab passwords do not meet the minimum length or alphanumeric requirements of the City password policy. SoftLab passwords are unnecessarily weak which is due to the fact SoftLab system passwords were configured several years ago, prior to the implementation of the current City's Password Policy, dated June 1, 2011.

Recommendation 4: Configure passwords to comply with the City's Password Policy.

Specifically, configure all SoftLab/SoftMic user passwords to meet the length and alphanumeric requirements of the City's password policy. The purpose of the policy is to establish a standard for the creation of strong passwords, protection of those passwords, and the frequency of changing passwords, and to protect information systems and data from unauthorized access.

Documented Periodic User-Access Reviews

For applications containing sensitive information, documented periodic reviews are performed to ensure appropriate access of personnel. User access to information systems with sensitive information should be reviewed and approved periodically to ensure system access is granted using least-privilege criteria, based on job responsibilities and approved by an authorized resource owner. Access should be disabled in a timely manner when employees are terminated.

SoftLab/SoftMic contains sensitive information. A documented periodic user-access review does not exist for these applications. User-access reviews have not been performed twice a year. Periodic system-access reviews are not documented, reviewed, or approved by the resource owner. The audit found that a terminated employee still had system access. The Laboratory's previous user-access updates were performed on an ongoing, as-needed basis, but they were not

documented or approved. However, the approach of a periodic, documented, and approved user-access review twice per year for applications that contain sensitive information is consistent with best practice. Thus, the Laboratory's own maintenance of applications that contain sensitive information and the standards imposed under HIPAA compel the Laboratory to elevate its best-practice measures to a level of periodic, documented, and approved user-access review.

Recommendation 5: Perform user-access reviews twice per year including the approval of the Laboratory Director.

The focus of the user-access review should be whether system access is granted using least-privilege criteria, which is based on job responsibilities. The person who performs the review should sign and date the document as the preparer. The documented evidence of a review and its approval should be the Laboratory Director's signature, along with the date, to be included on the revised user-access list. Additionally, the best-practice approach for applications that contain sensitive information is to perform the user-access review twice per year. The completed user-access reviews should be retained for three years.

C. System Configuration

AIX is an acronym for Advanced Interactive (X) Executive. AIX is an operating system manufactured by IBM that is based on a version of UNIX. AIX lies at the core of the Laboratory's operating environment and the foundation upon which all other application programs rely. The applications that depend on the AIX operating system are SoftLab, SoftMic, and SoftSec, along with the DB Vista database. It is up to the Administrator to establish initial security and maintain security through administrative actions.[4]

These applications scored high as critical applications to the City based on the Securance Risk Assessment for the City of Milwaukee, dated March 2012. The systems are used to track and report health and pandemic patterns for the City of Milwaukee's health trends.

[4] *IBM AIX V6 Redbook Advanced Security Features 2012*

The operating system security controls should restrict access to City IT resources and data. User ID timeout and lockouts should be enabled on the AIX operating system and applications. The IBM recommended configuration for AIX is 60 minutes for timeouts.

The audit noted the following:

- No user timeout configured for the AIX operating system (or emulator) root account as recommended under IBM security settings.
- No system inactivity timeout configured for SoftSec.
- The AIX operating system password is not required to be changed no matter how much time has passed.

The primary cause for this circumstance is that the AIX system security settings were configured several years ago with no user timeout for the root operating system account. This was the default setting from IBM upon delivery of the AIX operating system to the City.

Recommendation 6: Configure the software to the manufacturer's recommended settings. First, configure the AIX operating system (or emulator) user root account to initiate timeout after 60-120 minutes of inactivity, in accordance with IBM's recommended settings. Second, set the SoftSec system inactivity's timeout configuration to 30 minutes or less. Third, the AIX operating system password should be changed at least once per year.

D. Contingency Plan

HIPAA regulation requires covered entities to establish, maintain, and test contingency plans for their operations, as well as be prepared for business disruptions and disaster recovery events. The Contingency Plan section, in part, is located in section § 164.308(a) (7) (i) and states:

- *"Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and*

natural disaster) that damages systems that contain electronic protected health information."

The Contingency Plan standard includes five implementation specifications:[5]

1. Data Backup Plan (Required)
2. Disaster Recovery Plan (Required)
3. Emergency Mode Operation Plan (Required)
4. Testing and Revision Procedures (Addressable)
5. Applications and Data Criticality Analysis (Addressable)

Backup System Administrator

A Backup System Administrator has not been designated for the AIX and SoftLab systems. The current Administrator is the only employee able to perform the position's daily duties making it necessary to perform these duties while on vacation by logging on either from home or remote location. There are no other personnel available with the necessary technical skills to help meet peak work periods or act in the absence of the Administrator. Furthermore, a significant business disruption or disaster event could create an urgent need for a Backup System Administrator to sustain the Laboratory's critical applications and operations.

Recommendation 7: Designate and train a Backup System Administrator.

The designation of an appropriately skilled Backup System Administrator is an important component to an effective disaster-recovery plan and better enables the Laboratory to deal more effectively with peak work demands, business disruptions, or disaster-recovery events. Additionally, a Backup System Administrator could provide coverage and greater depth during the primary Administrator's vacation, absence or sick leave. Having a backup administrator is consistent with best practices.

[5] *Department of Health and Human Services – HIPAA Security Series 2009*

Contingency Plan Testing

The purpose of contingency planning is to establish strategies for recovering access to PHI should the City experience an emergency, or other similar occurrence, such as a power outage or disruption of critical business operations. The goal is to ensure that the City has its e-PHI available when needed and is able to meet the critical needs of various organizations that rely on laboratory testing. Covered entities are required to have a Contingency Plan § 164.308(a) (7). The Contingency Plan standard requires that covered entities:

- *"Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information."*

The mandatory Contingency Plan has not been tested. The plan may not be adequate to provide a basis to resume normal operations in a reasonable amount of time after a significant business disruption or disaster event. Testing of the contingency plan has not occurred due to the Laboratory experiencing a significant increase in its workload, as well as staff turnover.

Recommendation 8: Implement procedures for periodic testing and revision of Contingency Plans.

The Contingency Plan should be tested to determine whether the plan is adequate enough to provide a basis for resuming normal operations in a reasonable amount of time after a significant business disruption or disaster event. Disaster recovery and emergency-mode operations plans could be tested by using a scenario-based walkthrough (to avoid daily operations impacts) or by performing complete live tests.[6]

Server Room Fire Suppression

AIX and SoftLab are run on a City-owned server, located in a locked, secured room of a City owned facility. The operating system, software application, and database are all on one machine. The current fire suppression system in the Server Room, is a water sprinkler with a heat-sensor

[6] *Department of Health and Human Services – HIPAA Security Series 2009*

ignition. The water sprinkler is located directly above the server machine that contains the operating system, software applications, and database. In the event of an actual fire, the water sprinkler fire-suppression system could significantly damage or destroy the server and render the entire information system inoperable. A water-damage event would likely be costly for the City and take a substantial period of time for recovery.

Recommendation 9: Upgrade the water-based fire sprinkler above the server to a chemical-based fire suppression system.

A chemical-based fire suppression system for information technology hardware and software is consistent with best practice.

City of Milwaukee
Tom Barrett
Mayor
Bevan K. Baker, FACHE
Commissioner of Health
Health Department Office of the Commissioner
www.milwaukee.gov/health
Frank P. Zeidler Municipal Building, 841 North Broadway, 3rd Floor, Milwaukee, WI 53202-3653 phone (414) 286-3521 fax (414) 286-5990

February 27, 2014

Aycha Sirvanci, CPA
Audit Manager
City of Milwaukee Comptroller's Office
City Hall, Room 404

Dear Ms. Sirvanci:

Thank you for the opportunity to respond to your thorough audit of the AIX and SoftLab System Controls of our Laboratory Information System (LIS). The thoughtful and objective review conducted by your staff has targeted measures that will greatly assist us in our ongoing efforts to evaluate and improve upon the systems we currently have in place. Please find included below a summary of how we intend to respond to each of your recommendations.

Recommendation #1 – Identify and designate a Security Official.

The laboratory has designated a management position, the Laboratory Operations Manager, to oversee responsibilities for laboratory HIPAA security compliance within the capabilities of the Laboratory Division and the Health Department's HIPAA compliance policies. This individual will work closely with the Laboratory Director, Laboratory Information Systems (LIS) Specialist, and other staff to address MHD Laboratory HIPAA security issues for the laboratory. However, MHD Laboratory HIPAA compliance relies upon the greater context of Departmental HIPAA security compliance and therefore may be limited in its capability to respond to all issues which rely upon decisions at the Departmental or City level that also interact with and impact the secure operation of the IBM AIX operating system and the Laboratory Information System's applications, SoftLab and SoftMic. The laboratory therefore relies on ITMD to maintain interface security and other functions of the LIS. It is our recommendation that MHD Departmental Security compliance working with ITMD is essential to support the Laboratory Division efforts. The laboratory cannot maintain HIPAA compliance in isolation, given the complex nature and interactivity of the various levels of overlap among these entities related to the LIS. Also, our LIS Administrator has many other duties in addition to the LIS and relies on ITMD staff on a regular basis, as well as vendor expert assistance, to maintain and assure a secure and confidential system.

Implementation date: Completed February 2014

Recommendation #2 – Perform a HIPAA-compliant risk analysis and document the process and results.

The Laboratory, according to the HIPAA regulations cited in the audit, is to conduct a thorough assessment of risk and vulnerabilities to confidentiality, integrity and availability of electronic protected health information (PHI), in this case the LIS. Currently several facets of risk analysis are in place. However, the Laboratory agrees there is always room for improvement. For example, the LIS Administrator currently has a system in place to assure integrity of electronic data by reviewing a large sampling of data entry into the LIS on a daily basis and recording, correcting and reviewing with staff any discrepancies detected. Additional trends can be identified in this system that will measure risks to data integrity. Future additions to these efforts to review potential risks will include evaluating the likelihood and impact of potential risks to PHI, performing a direct observation to assess current HIPAA compliance, and identifying employee turnover and password maintenance schedules. After the assessment has occurred, we will measure and address identified risks, and document chosen security measures that include a rationale for adopting those measures.

Implementation date: December 2014

Recommendation #3 – Develop and implement a formalized quality-review process.

Several systems are in place currently to ensure security of data and PHI in the LIS. Multiple layers of security exist, including that the laboratory facility is secured by biometric access controls; access to the LIS is password-protected; the LIS is firewall-protected and contains special hardware recently updated to assure secure connections with the vendor through ITMD; the LIS is sourced by a private vendor and the software is vendor-specific and not generic. Laboratory staff currently, and for several years now, are mandated to undergo security training under federal guidelines of the Centers for Disease Control and Prevention's Select Agent Program. This program requires policies and annual training on electronic security and annual revisions of the MHD Laboratory Security Plan. The Laboratory also has a Corrective Action system in place such that when errors or problems are detected related to safety, security or quality, a Corrective Action Form is filled out, documented and reviewed by staff and management to prevent a repeat of the error or problem detected.

However, the Laboratory agrees that additional steps and processes can be put in place to enhance the quality review process. The Laboratory will develop and implement a formalized "spot check" quality-review process that will monitor and evaluate HIPAA at all Laboratory and Clinic service sites including MHDL and Keenan Health Center (KHC). Items to be spot checked for HIPAA compliance include requisition forms, LIS terminal screens and reports, and patient specimens.

Implementation date: December 2014

Recommendation #4 – Configure all - passwords to comply with the City's Password Policy.

As of February 24, 2014, the following changes have been enacted to comply with the City's Password Policy:

1. Password change required every 8 weeks	Hosparam: passwd_weeks = 8
2. Minimum length of 8 characters	Hosparam: PRule_Length = 8
3. At least one uppercase letter required	Hosparam: PRule_Uppercase = Y

4. At least one digit (number) required Hosparam: PRule_Numbers = Y

Special characters may be used but will not be required. Lowercase letters may also be used; however, the SCC Hosparam controlling this (PRule_Lowercase) was not in our current 4.0.1 software release. It was incorporated into the 4.0.2 release and will be a requirement when the Laboratory upgrades to the newest software release (currently 4.0.7.x).

Implementation date: Completed as of February 2014.

Recommendation #5 – Perform user-access reviews twice per year including the approval of the Laboratory Director.

A user-access review twice per year will be created as recommended. User access is currently strictly controlled as follows. When an LIS user account is created for an individual, that individual is only granted access to module options that are required for their job (i.e. "roles"). All user account access is set to expire on December 31 of the current calendar year. The user is notified 30 days in advance at login that their account is set to expire, and needs review by the LIS Administrator. Additionally, user account reviews shall be conducted twice per year (June, November), and documented with the Laboratory Director's signed approval.

Implementation date: December 2014

Recommendation #6 – Configure the software to the manufacturer's recommended settings. Firstly, configure the AIX operating system (or emulator) user root account to initiate timeout after 60-120 minutes of inactivity, in accordance with IBM's recommended settings. Secondly, set the SoftSec system inactivity's timeout configuration to 30 minutes or less. Thirdly, the AIX operating system password should be changed at least once per year.

1. Currently, the "root" level of the AIX operating system is accessed by the LIS administrator through specific UNIX commands using the PowerTerm emulator software application installed on the desktop PC or laptop. In the chance that the LIS administrator would forget to exit the "root" level, the PowerTerm emulator has been configured to terminate the application after a period of 60 minutes of inactivity.
2. The LIS Administrator (and the designated backup), are the only individual(s) that have access to the SoftSecurity module. The Security module is set to timeout the application after 10 minutes of inactivity.
3. SCC Soft Computer, the owner of the proprietary software used by the LIS, assigns the root password for the AIX operating system for the client site. At the MHD Laboratory, only the LIS Administrator has access to this password. When a backup to the administrator is selected, that person will also have access to the root password after sufficient training by the LIS Administrator. The root password shall be changed after any of the following:
    a. LIS Administrator leaves City employment for any reason
    b. LIS backup administrator leaves City employment for any reason
    c. Confirmed or successful attempts to access or penetrate the City's IT infrastructure (i.e. firewall) as determined by ITMD
    d. On an annual basis based on best practices.

Implementation date: Completed as of February 2014

Recommendation #7 – Designate a backup administrator.

A designated backup administrator will be identified to be trained by the current LIS administrator. This individual will commence training by May 1, 2014. In addition, the Laboratory Operations Manager will facilitate and assist with documentation and training of these duties. Training is anticipated to require a minimum one year, with a completion date by December 31, 2015.

Implementation date: December 2015

Recommendation #8 – Implement procedures for periodic testing and revision of contingency plans.

The laboratory will implement and test the current LIS Contingency Plan and determine the effectiveness of our strategies for resuming normal operations after a significant business disruption or disaster event. The goal will be to update and revise the plan based on the information gathered from this audit, and create documentation strategies that will be signed by the Laboratory Director and offered to staff via emergency training in-service.

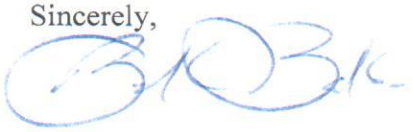
Implementation date: December 2014

Recommendation #9 – Upgrade the water-based fire sprinkler above the server to a chemical-based fire-suppression.

The Laboratory Operations Manager is in the process of scheduling meetings with DPW Facilities regarding the issue of the location of a water sprinkler in the data closet currently hosting the LIS servers. He will continue to work with DPW to incapacitate the water sprinkler and seek funds to address the recommendations as described.

Implementation date: December 2014

Sincerely,



Bevan K. Baker, FACHE
Commissioner of Health