COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

JOHN NAIMO
AUDITOR-CONTROLLER

April 20, 2015

TO: Supervisor Michael D. Antonovich, Mayor
Supervisor Hilda L. Solis
Supervisor Mark Ridley-Thomas
Supervisor Sheila Kuehl
Supervisor Don Knabe

FROM: John Naimo
Auditor-Controller

SUBJECT: **DEPARTMENT OF PUBLIC HEALTH – INFORMATION TECHNOLOGY AND SECURITY POLICIES REVIEW**

The Board of Supervisors' (Board) Information Technology (IT) and Security Policies (Policies) require all County departments to comply with established Countywide IT security standards to help ensure proper controls over County IT resources. As required by Board Policy 6.108, we are reviewing County departments' compliance with the Policies.

We have completed a review of the Department of Public Health's (DPH or Department) compliance with the Policies and related County standards. Our review included testing system access to five systems DPH identified as mission critical, including systems containing sensitive health information. We also reviewed physical security over IT equipment, computer encryption and antivirus software, equipment disposition, and IT security awareness training.

Results of Review

Our review disclosed that DPH needs to improve its controls over areas such as systems access, IT equipment control, and computer encryption. In addition, some of the issues noted could violate federal Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act laws. Therefore, we reported our preliminary findings to the County's Chief HIPAA Privacy Officer. The following are examples of areas for improvement:

- **Inappropriate Systems Access** – DPH needs to restrict unneeded access to sensitive/confidential information in their systems, and determine whether unneeded access resulted in a HIPAA/HITECH violation. We reviewed two of DPH's systems, and noted that DPH did not remove systems access for 13 users who terminated DPH employment. One of the terminated employee accounts was used for three years after the employee terminated to view protected health information (PHI) and to order laboratory tests for approximately 100 DPH clients. DPH management indicated that they are investigating to determine if the individual who accessed the terminated user account was authorized to view the PHI and to order the laboratory tests.

  DPH's attached response indicates they determined that a current employee used the terminated employee's account in performing her job duties. The current employee failed to obtain her own system account, which violated County policy. However, she was authorized to view PHI and no reportable HIPAA/HITECH violation occurred. DPH indicates it has reminded IT managers to promptly remove terminated employee access. DPH is also developing a procedure to notify managers of personnel changes so they can immediately update systems access.

- **Systems Access Documentation** – DPH needs to improve their systems access documentation. We could not review user access for three of DPH's systems. For one of the three systems, DPH could not generate a list that identifies who has access to the system. For two systems, DPH could not document system access role capabilities, making it impractical to determine if users' access roles were appropriate for their job duties.

  DPH's response indicates they implemented a system upgrade that allows them to generate user access logs to monitor system access. In addition, DPH will develop a system access authorization form that includes access role descriptions and justifications.

- **Physical Security** – DPH needs to physically secure its IT resources, as required by Board Policy 6.106. Twenty-one employees who terminated from the County continued to have key card access to enter three DPH offices for up to five years after termination. We also noted that DPH stores surplus computer equipment in a warehouse receiving area that is open to the public for deliveries. In addition, laptops at two (40%) of the five offices reviewed are not secured with a lock when left unattended.

  DPH's response indicates they canceled key card access for the terminated employees and will develop procedures to immediately update keycard access when personnel changes occur. DPH also convened an Asset Management

Improvement Team to ensure computer equipment in their warehouse and other facilities are properly secured.

- **Inaccurate IT Inventories** – DPH needs to improve controls over IT equipment inventories. We could not locate seven (10%) of the 68 items from DPH's equipment lists. While DPH staff indicated that some of these items had been disposed, they could not document any of the disposals. In addition, we noted 9,400 (45%) of the 20,757 items on DPH's lists have a missing or incorrect make/model, manufacturer's serial number, asset custodian, etc., including 315 items assigned to individuals who no longer work at the Department.

  DPH's response indicates they investigated and submitted a Computer Security Incident Report to the County Chief Information Security Officer for the missing IT devices. DPH also reminded managers and asset custodians to immediately report lost, stolen, or improperly inventoried IT resources. DPH's Asset Management Improvement Team is also reviewing inventory management procedures to identify improvements.

- **Staff Computer Assignments** – DPH needs to evaluate staff computer assignments, transfer/salvage unneeded items, and evaluate establishing a computer pool and checkout process for computer devices that staff do not frequently use. DPH's inventory records indicate that 487 (14%) of the 3,583 employees have two or more assigned computers (e.g., a desktop and a laptop or tablet). Eight (32%) of the 25 employees interviewed with two or more computers indicated they do not need one of their computers, including one employee who had not used his laptop for two years.

  DPH's response indicates they will review computer assignments to determine if the type and amount of devices are aligned with asset custodians' job duties. They will also evaluate expanding the use of computer check-out pools.

- **Portable Computer Encryption** – DPH needs to improve encryption documentation and ensure portable computers are encrypted, as required by Board Policy 6.110. DPH did not have encryption documentation for 319 (18%) of the 1,773 portable computers. In addition, their documentation for the remaining items does not include enough detail, such as the computers' asset tag or serial numbers, to match it to any of the 1,773 computers in inventory. We reviewed 28 portable computers and noted eight (29%) did not have encryption software installed. We also noted that staff/managers do not periodically monitor to ensure portable computers are encrypted.

  DPH's response indicates they will recall all portable computers to validate and document that each device is encrypted. DPH also worked with the Chief

Information Office to acquire software that will allow them to monitor the encryption status of all portable and desktop computers.

- **Antivirus Software** – DPH needs to ensure all computers have current antivirus protection, as required by Board Policy 6.102. Thirteen (23%) of the 56 computers reviewed had outdated antivirus software protection, including one computer with no antivirus software installed.

  DPH's response indicates they will review all portable computers to verify that antivirus protection is installed and configured to receive routine updates.

- **Hard Drive Disposal** – DPH needs to properly document that all County data is erased from hard drives when computers are disposed, as required by Board Policy 6.112. We noted two instances where DPH disposed of 65 hard drives but could not document erasing ten (15%) of them. In another instance, DPH documented disposing of 35 computers and four boxes of hard drives, and documented erasing 84 hard drives. However, DPH's documentation does not indicate how many hard drives were in the boxes, so we could not determine if DPH erased all hard drives before disposal.

  DPH's response indicates they implemented a new procedure where program offices send each computer to DPH's Materials Management warehouse for proper sanitation and documentation.

- **Computer Incident Response** – DPH needs to report missing IT equipment through the County's computer incident response process. We noted that between 2011 and 2013, DPH managers/staff failed to report 131 missing or stolen IT equipment items to the Department's Information Security Officer (DISO), as required by Board Policy 6.109. As a result, the DISO could not assess the impact of any data/software loss and could not make any required notifications to the Chief Information Office, the Auditor-Controller (A-C) HIPAA Privacy Officer, or the A-C Office of County Investigations.

  DPH's response indicates they have reminded all employees to immediately report missing or stolen IT resources to their supervisor. DPH management also told us that subsequent to our review, they investigated and accounted for 100 (76%) of the 131 missing IT equipment items. Of the 31 that remain unaccounted for, DPH indicated that three could have contained PHI, but DPH indicated they believe the risk of a breach is low. They are preparing a separate memo to the Board on this issue.

Details of these and other findings and recommendations are included as Attachment I.

Review of Report

We discussed our report with DPH management. The Department's attached response (Attachment II) indicates general agreement with our findings and recommendations.

We thank DPH's management and staff for their cooperation and assistance during our review. If you have any questions, please contact me, or your staff may contact Robert Smythe at (213) 253-0100.

JN:AB:RS:MP

Attachments

c: Sachi A. Hamai, Interim Chief Executive Officer
Cynthia A. Harding, M.P.H., Interim Director, Department of Public Health
Robert Pittman, Chief Information Security Officer, Chief Information Office
Linda McBride, Chief HIPAA Privacy Officer, Department of Auditor-Controller
Public Information Office
Audit Committee

DEPARTMENT OF PUBLIC HEALTH
INFORMATION TECHNOLOGY AND SECURITY POLICIES REVIEW

Background

The Board of Supervisors' (Board) Information Technology (IT) and Security Policies (Policies) require all County departments to comply with Countywide IT Policies, standards, and guidelines. The Policies help protect County IT assets and ensure the confidentiality and integrity of systems data. As required by Board Policy 6.108, we are reviewing County departments' compliance with the Policies.

We have completed a review of the Department of Public Health's (DPH or Department) compliance with the Policies, and related County standards and guidelines. DPH has approximately 21,000 IT devices such as desktop computers, laptops, servers, multifunctional printers, tablets, etc. Our review included testing systems access, physical security, encryption and antivirus software, equipment disposition, and IT security awareness training.

Systems Access

Board Policy 3.040 requires departments to safeguard personal and confidential information on their IT systems. As an entity that delivers health care and possesses protected health information (PHI), DPH is responsible for compliance with information security and privacy standards defined within the federal Health Insurance Portability and Accountability Act (HIPAA), including the Health Information Technology for Economic and Clinical Health (HITECH) Act. These laws address privacy and security requirements related to the storage and transmission of PHI, to prevent against unauthorized access and data breaches. Failure to comply with HIPAA and HITECH can result in practices or incidents that may be reportable to the United States Department of Health and Human Services.

Inappropriate Access

We reviewed user access for two of the 30 systems that DPH identified as mission critical. The systems reviewed were the Pharmacy Inventory and Labeling System (PILS), and the Public Health Laboratory System (PHLAB). Our review was intended to determine if access to PHI is limited based on employee job duties.

Based on our review, user access to PILS appeared to be appropriate. However, we noted that 13 PHLAB users, including two contractors, terminated employment/contracts with DPH but continued to have active access to PHLAB for two weeks to three years after termination. In addition, one of the user accounts was used to access PHLAB 133 times after termination to view PHI and order laboratory tests for approximately 100 clients. DPH management indicated they are investigating whether the individual who accessed the terminated user account was authorized to view the PHI and to order the laboratory tests.

These issues occurred because DPH staff did not follow Department policy for immediately restricting access when employees terminate, and did not periodically review PHLAB access levels, as required by County Fiscal Manual (CFM) Section 8.7.4.2.

DPH management needs to determine if the terminated employee's access to PHLAB resulted in a HIPAA/HITECH violation, and take action to correct and report any violations. The Department also needs to remind staff to immediately update systems access privileges when employees terminate and periodically review systems access to ensure access levels are authorized and appropriate for each user's job duties.

Recommendations

Department of Public Health management:

1. **Determine if terminated employee access to the Public Health Laboratory System resulted in a HIPAA/HITECH violation, and take action to correct and report any violations.**

2. **Remind staff to immediately update systems access privileges when employees terminate.**

3. **Periodically review systems access to ensure access levels are authorized and appropriate for each user's job duties.**

Access Documentation

We planned to review user access for three other critical DPH systems; the Patient Health Information System (P-HIS), CaseWatch HIV, and CaseWatch STD. However, we could not review access due to a lack of documentation. Specifically:

- **User Access Reports –** DPH could not generate a user access report for P-HIS. As a result, we could not identify who had system access or their access capabilities. DPH management indicated that P-HIS is a legacy system that does not currently have access reporting capability. DPH management needs to evaluate modifying the P-HIS to track and report user access roles, or develop alternative measures to monitor user access.

- **Access Role Documentation** – DPH could not document the user access role capabilities for the CaseWatch HIV and CaseWatch STD Systems. As a result, we could not determine if users' access roles are appropriate for their job duties. DPH management needs to document access role capabilities for CaseWatch HIV and CaseWatch STD, and monitor access as required.

Without sufficient information, the Department cannot adequately monitor user access and access role capabilities as required by CFM Section 8.7.4.2.

Recommendations

Department of Public Health management:

4. **Evaluate modifying the Patient Health Information System to track and report user access roles, or develop alternative measures to monitor user access.**

5. **Document access role capabilities for CaseWatch HIV and CaseWatch STD, and monitor access as required.**

Access Controls

Board Policy 6.101 requires systems to have appropriate user authentication such as log-on identifications (ID) and passwords that are not shared. CFM Section 8.7.4 includes password complexity requirements, and requires departments to document approvals for system access assignments.

We reviewed access controls for the five DPH systems mentioned in the sections above, and noted the following weaknesses:

- **Password Complexity** – Passwords for four (80%) of the five systems do not require a combination of numeric, upper, and lower case characters as required by the CFM.

- **Access Authorizations** – 18 (90%) of the 20 user accounts reviewed for four systems did not have documented approval for the access. This includes 16 users who had no access request form on file, and two users who had an access request form on file that was not signed by a supervisor. We could not review access authorizations for the fifth system due to the lack of a user access report noted in the section above.

DPH management needs to require systems passwords to include a combination of numeric, upper, and lower case characters, and needs to document approvals for all system access assignments.

Recommendations

Department of Public Health management:

6. **Require systems passwords to include a combination of numeric, upper, and lower case characters.**

7. **Document approvals for all system access assignments.**

Physical Security

Board Policy 6.106 requires departments to physically safeguard IT resources from tampering, damage, theft, or unauthorized physical access. This includes developing a Facility Security Plan that documents the physical security measures at each facility. These controls help prevent data breaches such as the recent breach at a DPH contractor.

We noted that DPH has not developed Facility Security Plans. In addition, we visited five DPH offices that house critical IT resources such as data centers, computers, multifunctional printers, etc., and noted the following physical security weaknesses:

- **Inappropriate Access:** Twenty-one employees who terminated from the County continued to have active key card access to enter three DPH offices for up to five years after termination.

- **Unsecured Equipment:** DPH staff do not always secure unattended computer equipment. Specifically, DPH's Materials Management Division stores surplus computer equipment in a warehouse receiving area that is open to the public during business hours. DPH staff are not always present, making the equipment, data, and software susceptible to theft. In addition, laptops at two of the five DPH offices reviewed are not secured with a lock when left unattended.

- **Surveillance System:** One of DPH's most critical data centers containing confidential data has a surveillance system that does not work. DPH IT managers are aware of the issue, but need to take action to identify funds and dedicate staff to replace the surveillance system.

DPH management needs to immediately cancel key card access for the terminated employees noted in our review and for any employee who transfers locations or terminates. DPH also needs to secure unattended computing devices when not in use, including when devices are waiting for sanitation and disposal. While Board Policy does not require surveillance cameras, DPH needs to identify funds and staff resources to replace the surveillance system at the critical IT facility identified in our review.

Recommendations

Department of Public Health management:

8. **Immediately cancel key card access for the terminated employees noted in our review, and for any employee who transfers locations or terminates.**

9. **Secure unattended computing devices when not in use, including when devices are waiting for sanitation and disposal.**

10. Identify funds and staff resources to replace the surveillance system at the critical information technology facility identified in our review.

IT Equipment Control

Board Policy 6.106 requires departments to assign IT equipment to specific individuals (custodians). CFM Chapter 6 also requires departments to inventory their IT equipment annually and to keep up-to-date IT equipment lists. These controls help ensure County computers and data are accounted for and safeguarded.

Equipment Inventories

We reviewed 98 DPH IT equipment items, including the 68 from DPH's equipment lists and 30 we observed at five DPH field offices. We noted missing IT equipment, and weaknesses in equipment control that could allow County computers and data to go missing or be stolen without being detected. Specifically:

- **Missing Equipment** – We could not locate seven (10%) of the 68 items from DPH's equipment lists. This includes three desktops, two laptops, and two tablets assigned to DPH offices that manage PHI. DPH IT staff at one office indicated that five of the computers may have been disposed, but could not provide any disposal documentation. DPH management needs to investigate the missing computer devices and report any lost or stolen computers through the County's incident response procedures to minimize the risk of any lost data or software on these devices.

- **Inaccurate Tracking** – 40 (41%) of the 98 items reviewed had an inaccurate custodian, location, or equipment description recorded on DPH's equipment lists. Using audit software, we analyzed all 20,757 items on DPH's IT equipment lists and noted that 9,400 (45%) have a missing or incorrect make/model, manufacturer's serial number, asset custodian, etc., including 315 items assigned to individuals who no longer work at the Department. DPH needs to update its equipment inventories for the inaccuracies identified in our review.

- **Asset Tags** – DPH generally does a good job of using asset tags to account for IT equipment. However, we noted one (1%) of the 98 IT equipment items reviewed did not have an asset tag to identify it as County property. DPH needs to ensure a County property tag is attached to all equipment.

We also noted DPH does not properly conduct physical inventories of their IT equipment because they do not always update their inventory lists for discrepancies in location, custodian, or equipment description when conducting their physical count. DPH needs to conduct accurate physical inventories and investigate and update inventory lists for any discrepancies.

Recommendations

Department of Public Health management:

11. **Investigate missing computer devices and report any lost or stolen computers through the County's incident response procedures.**

12. **Update equipment inventories for the inaccuracies noted in our review.**

13. **Ensure a County property tag is attached to all equipment.**

14. **Ensure staff conduct accurate physical equipment inventories and investigate and update inventory lists for any discrepancies.**

Computer Assignments

DPH's records indicate that 487 (14%) of their 3,583 employees have two or more computers assigned to them (e.g., a desktop and laptop or tablet). Eight (32%) of the 25 staff interviewed with two computers indicated that they do not need one computer, including one person who had not used his laptop for two years. In addition, three of the eight individuals had two of the same type of device (e.g., two laptops, two tablets, etc.). Unneeded computers increase the risk of loss, and result in higher maintenance, support, and software costs.

DPH should evaluate their staff computer assignments, transfer or salvage unneeded items, and evaluate establishing a computer pool and checkout process for devices that staff do not frequently use.

Recommendation

15. **Department of Public Health management evaluate staff computer assignments, transfer or salvage unneeded items, and evaluate establishing a computer pool and checkout process.**

Portable Computer Encryption

Board Policy 6.110 requires departments to encrypt all County owned portable computers. Encryption helps render data unreadable if a computer is lost or stolen, and protects against unauthorized disclosure of personal/confidential information.

DPH could not document that they encrypted all of the 1,773 portable computers in their inventory. Specifically, DPH only had encryption documentation for 1,454 (82%) portable computers (319 less than their inventory). In addition, the encryption documentation did not include enough information, such as each device's asset tag number or serial number, to allow us to match it to any of the 1,773 computers in

inventory. We reviewed 28 portable computers assigned to DPH staff and noted eight (29%) did not have encryption software installed. In addition, DPH management does not periodically monitor the Department's portable computers to ensure that each device is encrypted.

DPH needs to ensure all portable computers are encrypted, and that each portable computer can be specifically matched with documentation that confirms it is protected by current encryption technology, and periodically monitor the encryption status of all portable computers.

Recommendations

Department of Public Health management:

16. **Ensure all portable computers are encrypted, and that each portable computer can be specifically matched with documentation that confirms it is protected by current encryption technology.**

17. **Periodically monitor the encryption status of all portable computers.**

Antivirus Software

Board Policy 6.102 requires departments to ensure they have functioning up-to-date antivirus software protection for all County computers. Departments must update antivirus software regularly to protect against the most current threats.

Thirteen (23%) of the 56 computers reviewed did not have up-to-date antivirus software protection, including one with no antivirus software installed. DPH management needs to ensure all computers have current antivirus protection.

Recommendation

18. **Department of Public Health management ensure all computers have current antivirus protection.**

Hard Drive Disposal

Board Policy 6.112 requires departments to render unreadable and unrecoverable all data and software from computer hard drives before disposing of the devices from County inventory.

We reviewed ten instances where DPH disposed of multiple computers and hard drives. For three (30%) of the ten computer disposals reviewed, DPH could not document that they erased every hard drive disposed. Specifically:

- In two disposal instances, DPH could not document erasing ten (15%) of the 65 total hard drives.
- In one disposal instance, DPH documented disposing of 35 computers and four boxes of hard drives, and documented erasing 84 hard drives. However, we could not determine if DPH erased every hard drive because the documentation does not indicate how many hard drives were in the boxes.

DPH also does not document the asset tag number of disposed computing devices or the serial number of the erased hard drives, making it impossible to determine which computing devices had their hard drive erased. DPH management needs to ensure all hard drives are properly erased before disposal, maintain documentation of the erasures, and ensure the documentation includes the serial number and/or computing device asset tag number of every hard drive erased.

Recommendation

19. Department of Public Health management ensure all hard drives are properly erased before disposal, maintain documentation of the erasures, and ensure the documentation includes the serial number and/or computing device asset tag number of every hard drive erased.

IT Security Incidents

Board Policy 6.109 requires department management to immediately report IT security incidents through the County's computer incident response procedure to minimize the impact of security breaches, such as HIPAA data loss, to individuals and to the County.

We noted that DPH does not always report IT security incidents through the County's incident response procedure. Specifically, DPH managers/staff identified 131 missing or stolen IT equipment items between 2011 and 2013, but did not report them to the Department Information Security Officer (DISO), as required by Board Policy 6.109.

As a result, the DISO could not assess the impact of these losses to the individuals, the Department, and the County. The DISO also could not make required notifications to the Chief Information Office, the Auditor-Controller's (A-C) HIPAA Privacy Officer, and the A-C Office of County Investigations that the items and any associated data or software were missing. Approximately 85 (65%) of the 131 missing/stolen items were assigned to sections that handle PHI, increasing the risk that HIPAA or HITECH violations could have occurred. DPH management needs to report missing and stolen computers through the County's incident response procedure, and remind staff to report security incidents to the DISO.

Weaknesses in DPH's security awareness training program, discussed in the next section, may have contributed to staff and managers' lack of knowledge of incident response procedures.

Recommendation

20. Department of Public Health management report missing and stolen computers through the County's incident response procedure, and remind staff to report security incidents to the Department Information Security Officer.

Information Security Training

Board Policy 6.111 requires departments to provide information security awareness training (Training) to all IT resource users at the time they are hired and periodically thereafter. Training should be documented to assist management in determining employee awareness and participation.

DPH management indicated that they provide periodic Trainings for all IT users, but also indicated that the training is optional, generates low attendance, and DPH does not keep attendance records to evaluate employee awareness. DPH needs to ensure all IT resource users receive adequate IT Security Awareness Training.

DPH also could not document what Training material they provided to staff, so we could not determine if the Training addressed critical topics such as procedures for reporting IT security incidents as mentioned above. DPH needs to ensure IT training and attendance is documented.

Recommendation

21. Department of Public Health management ensure all information technology (IT) resource users receive adequate IT Security Awareness Training, and that the training and attendance is documented.

CYNTHIA A. HARDING, M.P.H.
Interim Director

JEFFREY D. GUNZENHAUSER, M.D., M.P.H.
Interim Health Officer

313 North Figueroa Street, Room 708
Los Angeles, California 90012
TEL (213) 240-8156 • FAX (213) 481-2739

www.publichealth.lacounty.gov

April 2, 2015

TO: John Naimo
Auditor-Controller

FROM: Cynthia A. Harding, MPH
Interim Director

Cynthia A. Harding

SUBJECT: **DEPARTMENT OF PUBLIC HEALTH – RESPONSE TO INFORMATION TECHNOLOGY AND SECURITY POLICIES REVIEW**

Please find attached our response to the audit performed by your department of Public Health's compliance with the Board of Supervisors' Information Technology and Security Policies.

As indicated in the attachment, DPH agrees with all of the findings and we are in the process of addressing those areas where we were not in full compliance. Our Departmental Information Security Officer will be following up to ensure that each corrective action is effectively implemented.

I would like to thank you and your staff for bringing to our attention the areas that we need to strengthen.

If you have any questions or require additional information, please contact me, or your staff may contact Jim Green, DPH Chief Information Officer, at 323.869.8179 or jimgreen@ph.lacounty.gov.

CH:JG:dc:av

Attachment

c: County Counsel
County Chief HIPAA Privacy Officer
County Chief Information Security Officer
Auditor-Controller
DPH Administrative Deputy
DPH Chief Information Officer
DPH Audit & Investigations Division
DPH HIPAA Privacy Officer
DPH Information Security Officer

Attachment I

Review of Public Health's Compliance with Board IT Policies

Systems Access

Inappropriate Access Recommendations

1. **Terminated Employee Access**

   Determine if terminated employee access to the Public Health Lab System resulted in a Health Insurance Portability and Accountability Act and Health Information Technology for Economic and Clinical Health Act Laws (HIPAA/HITECH) violation, and take action to correct and report any violations.

   Agree. DPH determined that the terminated employee's Public Health Lab System account was used by an employee assigned to perform the same duties that the terminated employee performed. The employee failed to obtain and use her own credentials for these duties, which violated County policy. However, this did not result in a reportable breach of Electronic Protected Health Information (ePHI). DPH reviewed Public Health Lab System user accounts at the health center to ensure that employees are all using their own credentials. The DPH IT Security Awareness Training Program includes a review of Acceptable Use. IT Security is emphasizing in each training session at DPH Program offices the requirement that employees use only their own authorized credentials for system access.

2. **System Access Privileges**

   Remind staff to immediately update systems access privileges when employees terminate.

   Agree. Since July, 2014, DPH IT Directors are being reminded in the Departmental Information Security Steering Committee to promptly remove credentials of terminated employees and to regularly review user accounts to ensure that all system access privileges are appropriate. DPH is developing procedures for notifying Program Directors and System Managers of personnel changes, instructing them to immediately update system access privileges when employees terminate or change assignments, and providing regular review of account privileges.

3. **Review of System Access**

   Periodically review systems access to ensure access levels are authorized and appropriate for each user's job duties.

   Agree. DPH now automatically disables any Active Directory account for which 60 days passes without login activity. The Departmental Information Security Officer is developing tools to conduct regular assessments of accounts and access privileges for each DPH system to ensure users have the appropriate level of access relative to their job duties.

Access Documentation Recommendations

4. <u>User Access Reports</u>
Evaluate modifying the Patient Health Information System (P-HIS) to track and report user access roles or develop alternative measures to monitor user access.

Agree. As part of an upgrade implemented in December 2014, users are now required to authenticate through Active Directory (AD) to log in to P-HIS. The login creates a user access log entry, which is being used to monitor access.

5. <u>Access Role Documentation</u>
Document access role capabilities for CaseWatch HIV and CaseWatch STD, and monitor access as required.

Agree. As of September, 2014, Casewatch (HIV) and STD*Casewatch users log in through Terminal Server. This login process creates a user access log entry, which is used to monitor access.

DPH will develop a standard System Access Authorization form by June 30, 2015, to include justifications for access and role descriptions for each system access request.

Access Controls Recommendations

6. <u>Password Complexity</u>
Require systems' passwords to include a combination of numeric upper and lowercase characters.

Agree. The DPH Active Directory, which controls access to PCs, file shares, and other DPH network resources, enforces complex passwords. Some DPH data systems require additional credentials for access, and we are conducting an evaluation to determine for each system whether it can be configured or modified to implement complex password requirements. In cases where strong password logic cannot be implemented, DPH will evaluate options to replace systems or provide compensating controls.

7. <u>Access Authorizations</u>
Document approvals for all system access assignments.

DPH will develop a standard System Access Authorization form by June 30, 2015, to include justifications for access and role descriptions for each system access request, and develop record-keeping procedures.

Physical Security

Physical Security Recommendations

8. Inappropriate Access

Immediately cancel keycard access for terminated employees and for any employee who transfers to another location or terminates employment.

Agree. DPH has canceled keycard access for terminated employees identified in the audit. DPH will develop procedures to notify Program Directors and System Managers of personnel changes and instruct them to immediately update keycard access when employees terminate or change assignments. We will also conduct periodic reviews of access lists to ensure that all access continues to be appropriate.

9. Unsecured Equipment

Secure unattended computing devices when not in use, including when devices are waiting for sanitation and disposal.

Agree. DPH has convened an Asset Management Improvement Team to work with the Ferguson Warehouse Managers and Asset Custodians to ensure that assets in the warehouse and other facilities are properly secured.

10. Surveillance System

Identify funds and staff resources to replace the surveillance system at the critical information technology facility identified in our review.

Agree. DPH has engaged a vendor to review the surveillance system and make recommendations for the design and implementation of a replacement system. Once a design is approved, DPH will move expeditiously to acquire and implement the replacement system.

To further address physical security, DPH will develop a Facility Security Plan to document physical security measures at each DPH facility.

IT Equipment Control

Equipment Inventories Recommendations

11. Missing Equipment

Investigate missing computer devices and report any lost or stolen computers using the County's incident response procedures.

Agree. DPH investigated the missing devices identified in the audit. A Computer Security Incident Report Form has been completed and submitted to the County Chief Information Security Officer in accordance with the County's incident response procedures.

Program Directors and Asset Custodians have been reminded that the County's incident response procedures require employees to report lost, stolen, or improperly inventoried County IT resources immediately to their supervisors. The monthly Departmental Information Systems Security Committee (DISSC) Meeting is used to periodically remind IT Directors of these requirements. In addition, at each annual inventory, the Departmental Information Security Officer will work with DPH Materials Management to ensure that in the event any computer items are not accounted for, they are properly reported using the DPH Computer Security Incident Report Form.

12. Inaccurate Tracking

Update equipment inventories for inaccuracies.

Agree. The DPH Asset Management Improvement Team is reviewing all inventory management procedures to identify gaps and prioritize improvements. Initial improvements include: (1) Salvage activities have been centralized for improved accuracy and control, and (2) PC technicians use the Department's barcode asset management system to immediately update inventory in the field as equipment is moved or salvaged.

13. Asset Tags

Ensure a County property tag is attached to all equipment.

Agree. DPH revised its process in December 2014 to ensure that all equipment received goes through the DPH Materials Management Warehouse, where it is tagged. In addition, PC technicians will be trained to ensure a County asset tag is attached when performing annual inventories, conducting routine inspections, providing maintenance, or replacing IT equipment.

14. Physical Inventories

Ensure staff conduct accurate physical equipment inventories and investigate and update inventory lists for any discrepancies.

Agree. The DPH Asset Management Improvement Team is reviewing all inventory management procedures to identify gaps and prioritize improvements. PC technicians will receive additional training on procedures and will use the Department's barcode asset management system to immediately update inventory in the field as equipment is maintained, moved or salvaged.

Computer Assignments Recommendation

15. Computer Assignments

Evaluate staff computer assignments, transfer or salvage unneeded items, and evaluate establishing a computer pool and checkout process.

Agree. DPH will evaluate current computer assignments to determine whether the appropriate equipment and the number of assigned computers are in alignment with job duties. We will ensure that proper transfer and salvaging of unneeded items are completed and documented. We will evaluate expanding the use of computer pools and refining the computer checkout process.

Portable Computer Encryption

Portable Computer Encryption Recommendations

16. Encrypt Portable Computers

Ensure all portable computers are encrypted and that each portable computer can be specifically matched with documentation that confirms it is protected by current encryption technology.

Agree. DPH will conduct a 100% recall of all portable computers in the Department to validate and document that they are properly encrypted. In addition, as part of the desktop encryption project, we are implementing the capability to monitor and report on the encryption status of all computers, including portables.

17. Monitor Encryption Status

Periodically monitor the encryption status of all portable computers.

Agree. DPH worked with the County Chief Information Security Officer to acquire WinMagic software, which DPH will use to monitor and report on encryption status of all desktops and portable computers.

Antivirus Software

Antivirus Recommendation

18. Ensure all computers have current antivirus protection.

Agree. The Department's desktop computers receive antivirus updates through routine patching over the network. As part of the portable computer recall, DPH will review each portable computer to verify its antivirus protection and correct each deficiency. We will ensure each computer is configured to receive routine antivirus updates.

Hard Drive Disposal

19. Proper Disposal of Hard Drives Recommendation
Ensure all hard drives are properly erased before disposal, maintain documentation of the erasures, and ensure the documentation includes the serial number and/or computing device asset tag number of every hard drive erased.

Agree. Previously, hard drives were removed from computers in DPH Program offices before being salvaged, which made it difficult to determine whether the hard drive was properly erased prior to disposal of the computer. Under our new procedures implemented in July 2014, the entire computer is sent to the DPH Materials Management Warehouse for proper sanitizing and documentation.

IT Security Incidents

20. Report Missing and Stolen Computers Recommendation
Report missing and stolen computers through the County's incident response procedure and remind staff to report security incidents to the Department Information Security Officer (DISO).

Agree. All DPH staff were reminded in March, 2015, that the County's incident response procedures require employees to report missing or stolen County IT resources immediately to their supervisors. The Departmental Information Security Officer routinely reinforces incident response procedures in the monthly Departmental Information Systems Security Committee (DISSC) Meeting.

Information Security Training

21. IT Security Awareness Training Recommendation

Ensure all information technology (IT) resource users receive adequate IT Security Awareness Training and that the training and attendance is documented.

Agree. Currently, Departmental policy requires that all employees take HIPAA awareness training within 30 days of employment. The Department's orientation package includes additional information about computer security. Effective May 2011, attendees of the quarterly IT Security Awareness Trainings sign in to document their attendance training. In addition, the Departmental Information Security Officer is working with the County Information Security Officer on selection and implementation of online IT security awareness training to be delivered to all employees through the LearningNet.