MIAMI-DADE COUNTY BOARD OF COUNTY COMMISSIONERS

OFFICE OF THE COMMISSION AUDITOR

AUDIT OF INTERNAL CONTROLS FOR THE PROTECTION OF ELECTRONICALLY STORED PERSONAL AND HEALTH INFORMATION:

Miami Dade Department of Human Services
(Currently a part of Community Action and Human Services Department)

Project Number 11-143370

October 11, 2012

Charles Anderson, CPA
Commission Auditor

Auditors

Michael O. Bayere, CIA, CISA, CISSP	Auditor-In-Charge
Norma Roig, CPA, CGMA	Senior Auditor
Noel Aranha, CPA, CGMA	Acting Audit Manager

111 NW First Street, Suite 1030
Miami, Florida 33128
305-375-4354

THIS PAGE INTENTIONALLY BLANK

BOARD OF COUNTY COMMISSIONERS
OFFICE OF THE COMMISSION AUDITOR

M E M O R A N D U M

TO: Honorable Joe A. Martinez, Chairman
And Members, Board of County Commissioners

FROM: Charles Anderson, CPA
Commission Auditor

DATE: October 11, 2012

SUBJECT: Audit of Internal Controls for the Protection of Electronically Stored Personal and Health Information (*former Department of Human Services)*

We have concluded our Audit of Internal Controls for the Protection of Electronically Stored Personal and Health Information for the former Department of Human Services (now part of Community Action and Human Services Department) and submit this report which contains findings, recommendations, and management response. Management concurred with all of our findings and recommendations.

We thank the staff of Internal Services, Information Technology Department, and Community Action and Human Services for their cooperation and input throughout the review. Please let me know if you need further information.

c: Mayor Carlos Gimenez, County Mayor
Russell Benford, Deputy Mayor, Office of the Mayor
Lucia Davis-Raiford, Executive Director, CAHSD
R. A. Cuevas, Jr., County Attorney
Chris Mazzella, Inspector General
Cathy Jackson, Director, Audit and Management Services
Angel Petisco, Director, Information Technology Department
Phyllis Tynes-Saunders, Assistant Director, CAHSD
Alberto Parjus, Assistant Director, CAHSD
Richard W. Harris, Director, Human Services Division, CAHSD
Lars Schmekel, Chief Security Officer, Information Technology Department
Delia A. Iglesias, Supervisor, Information Technology Unit, CAHSD

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY BLANK

I. OBJECTIVES AND SCOPE

As part of the work plan approved by the Miami-Dade County Board of County Commissioners (BCC), the Office of the Commission Auditor (OCA) conducted the Audit of Internal Controls for the Protection of Electronically Stored Personal and Health Information at the former Miami-Dade Department of Human Services (DHS). DHS is now part of Community Action and Human Services Department (CAHSD). The objectives of the audit were to assess the adequacy and operational effectiveness of physical, administrative and technical controls designed for protecting the confidentiality and integrity of personally identifiable and health information of DHS clients (programs applicants/participants). The scope of the audit was from October 1, 2010 through December 31, 2011.

II. METHODOLOGY

We conducted this audit in accordance with Generally Accepted Government Auditing Standards (GAGAS) and IT Audit and Assurance standards (*issued by ISACA*), except for section 3.82 (b) of GAGAS which requires audit organizations to obtain an external peer review at least once every three years. Those standards require that we plan and perform the audit to obtain sufficient, reliable, relevant and appropriate evidence to provide a reasonable basis for our findings and conclusion based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusion based on the audit objectives.

To accomplish our objectives, we identified all DHS services/programs, and reviewed processes for the collection, processing, transmission, storage, and disposal of programs participants' information that are considered confidential. We identified relevant regulations, statutes, standards and acts that applied to DHS programs with respect to information security. We identified all the major systems (applications and databases) the department uses in its processes, and performed risk analysis of the processes and systems to determine our audit tests.

Our audit tests included a review of physical controls for safeguarding records and electronic media containing confidential information across the department; and tests of security controls incorporated into computer applications and databases for those applications and databases managed and maintained either by DHS or by the Miami Dade Information Technology Department (ITD). We reviewed network security controls for protecting DHS computer network systems. We also used commercial vulnerability assessment software[1] to perform vulnerability assessment on critical servers (centralized, high-capacity computers serving other computers) and a sample of user computers (workstations). Due to access restrictions, we did not perform detailed security review of applications and databases used by DHS but are owned, maintained and administered either by the State of Florida or the Federal government.

In addition, we interviewed key personnel and assessed information security physical and administrative controls in fifteen (15) DHS sites across the County, and in other centralized units in the administrative office. We reviewed relevant County administrative orders, DHS and ITD information security policies, administrative procedures and other related records.

[1] Software specifically developed to identify and report on security weaknesses in computer systems

We benchmarked our security controls tests with the security requirements of applicable regulations, statutes, and acts (including HIPAA[2], the Privacy Act of 1974, Title 42 CFR[3] Part 2, and Title 5 Chapter 39[4] of Florida Statutes); and with recommended information systems security controls[5] by the National Institute of Standards and Technology (NIST).

III. BACKGROUND

DHS provides comprehensive county-wide social and human services to the residents of Miami Dade County. Services provided include those for children, the elderly, persons with disabilities, veterans, new immigrants and refugees, farmworkers, victims of domestic violence, and substance abuse patients.

DHS services/programs were organized into four administrative bureaus (divisions), namely: Child Development Services Bureau (CDS); Elderly, Disability and Veterans Services Bureau (EDVSB); Rehabilitative Services Bureau (RSB); and Targeted Services Bureau (TSB). DHS is now a part of Community Action and Human Services Department (CASHD).

Child Development Services Bureau (CDS) provides subsidized financially assisted School Readiness and Voluntary Pre-kindergarten (VPK) services for children from infancy up to nine (9) years of age; developmental screening and assessment services; resource and referral information on child-related services; training and technical assistance for child care providers; and payment services for School Readiness/VPK providers.

Elderly, Disability and Veteran Services Bureau (EDVSB) provides comprehensive services to elderly and young adults with disabilities (including adult day care, home care, meals on wheel, volunteer services); and technical assistance to veterans and their families in filing claims to the Veteran Service Administration.

Rehabilitative Services Bureau (RSB) provides substance abuse treatment and intervention services through assessment and referral for sentenced offenders and diverted drug offenders. It also provides residential treatment services to homeless adults and indigent individuals.

Targeted Services Bureau (TSB) offers crisis intervention and assistance to victims of violent crimes and domestic violence, provides clinical services to children participating in Head Start and Early Start programs; offers assistance services to newly arrived refugee youths and families; and administers employment program for at-risk youths (ages 18-25) who reside in Districts two (2) and three (3). TSB also provides vocational and employment related services to seasonal farmworkers.

Across the spectrum of services DHS offers to the residents, information deemed to be personally identifiable is collected from service recipients. DHS also generates and/or processes health information (relating to diagnosis, treatments etc.) in some of its services and programs.

[2] Health Insurance Portability and Accountability Act of 1996
[3] Code of Federal Regulations on Confidentiality of Alcohol and Drug Abuse Patients Records
[4] Proceedings Relating to Children
[5] Recommended Security Controls for Federal Information Systems and Organizations (NIST SP 800-53 Rev 3)

Personally Identifiable Information (PII) is any information that can be used (either alone or in combination with other information) to uniquely identify, trace or locate an individual. Examples include social security number, driver license number, passport number, credit card number, full name and mother's maiden name, date and place of birth, biometrics (e.g. fingerprints).

Because of the confidentiality and sensitivity of CAHSD information, sound information security is mandatory to safeguard the confidentiality and integrity of this information, and to ensure compliance with applicable regulations, statutes, and acts (such as HIPAA, The Privacy Act of 1974, Title 42 CFR Part 2, and Title 5 Chapter 39 of Florida Statutes). The responsibilities for protecting sensitive and confidential information in CAHSD rest not only on the department (CAHSD), but also on the Information Technology Department (ITD) because ITD provides certain centralized computing and security services to the department.

IV. SUMMARY RESULTS

Overall, we found that in order to better protect the confidentiality and integrity of information in CAHSD, improvements are needed in the following areas:

- Department uses wireless local area network (WLAN)[6] implemented with poor security features that can easily compromise confidential and sensitive information.
- Communication link between external users and the County internal network for one important application (computer program) used in the Child Development Bureau was not protected with appropriate security mechanisms.
- Policies for managing computer users' passwords on department/County computing resources were weak.
- Access rights of some former and transferred employees were not removed from the Social Services Information System (SSIS) and the Enhanced Field System (EFS) for months/years after the employees had been separated or transferred.
- Processes for fixing software defects and managing computers security settings failed to provide effective remediation of flaws and vulnerabilities in computer systems.
- There was no policy for secure use of removable storage media, and no documentations to provide evidence of secure sanitization or destruction of old electronic storage media.
- Policy for secure custody of clients' files/records was violated in two of the DHS sites we visited.
- Department did not have policy or guidelines to ensure that user-developed databases[7] and spreadsheets containing clients confidential information are secured with appropriate security mechanisms.

For security reasons, certain specific information about the audit findings is excluded from this report. This information was provided to the management of the department and ITD in a separate appendix (*Appendix I*), which is considered sensitive and exempt from public records, in accordance with Chapter 119.071(1) (f) of Florida Statutes.

[6] Network of computers linked together via wireless technology
[7] Repositories of electronic records

V. FINDINGS AND RECOMMENDATIONS

Finding 1.
Department uses wireless local area network (WLAN) implemented with poor security features that can easily compromise confidential and sensitive information (*Appendix I # T.1*).

The department's WLAN is part of the legacy wireless local area network deployed by the Information Technology Department (ITD) across County departments. The legacy WLAN employed what is known as Wired Equivalent Privacy (WEP) security to protect transmitted information. However, WEP is well-known to have inherent security flaws that can easily be exploited by attackers to intercept and compromise information being transmitted on the network. Information that can be compromised includes user login credentials, sensitive systems information, and other confidential information. The National Institute of Standards and Technology (NIST) says the following concerning one of the inherent weaknesses of WEP: "*WEP suffers from a number of cryptographic weaknesses that enable attackers with readily available software tools to decipher captured data, sometimes with as little as a few minutes of recorded traffic*[8]*".*

Good security practice and relevant information security standards (including HIPAA of 1996, PCI DSS, and NIST SP800-53) require the implementation of appropriate security controls to protect confidentiality and integrity of information during transmission.

Recommendations
a. ITD should upgrade wireless local area network (WLAN) to one based on security standards with robust security features (e.g. Wi-Fi Protected Access II (WPA2)).
b. ITD should establish effective risk assessment and control processes to continuously manage the risks of wireless network.

Management Response
CAHSD concurs with this finding and responds to the recommendations as follows:

a. CAHSD requested that ITD's Field Services Division provide an estimate for implementation of wireless security. ITD, working closely with CAHSD completed the estimate as requested. An implementation plan will be created based on the assessment and estimate. Historically, network equipment located at departmental sites was purchased by departments, either as part of the initial deployment or purchased as needed to replace aging, unsupported equipment. Support and maintenance of the original equipment was provided by ITD. The purchase of replacement equipment as part of modernization or upgrade of the network was funded by departments and implemented by ITD. Recently, ITD adopted a new support model whereby aging network equipment is replaced with newer equipment providing additional functionality and security. The purchase, maintenance and recapitalization of the equipment is now included in a monthly "port charge" of $10.00/active port. A port is defined as the point

[8] NIST Special SP 800-97 – Establishing Wireless Robust Security Networks (p.3-9)

where a network device (computer/server/printer) is connected to the County's network. The annual service charges include deployment, configuration, management and recapitalization/replacement of the network equipment. This updated business model ensures that each participating department's network will remain current, state of the art, supported and secure.

b. *ITD will develop an effective risk assessment and control processes to continuously manage the risks of wireless network. This will be completed within 90 days after the wireless security implementation plan is approved. The new equipment being proposed for deployment (and associated port charges) is part of the Edge Network Infrastructure project which will update network infrastructure throughout the County. This project was intended to modernize the County's network as well as improve wired and wireless security to meet current standards and best practices. This new infrastructure for both wired and wireless connectivity will be managed centrally by ITD and the risk management process will be integrated as part of the overall management of the network. Although CAHSD was not included in the 2012/13 deployment plan, the department and associated sites will be expedited and should be completed by March 2013.*

Finding 2.
Communication link between external users and the County internal network for one important application (computer program) used in the Child Development Bureau was not protected with appropriate security mechanisms *(Appendix I # T.2).*

The application (name withheld for security reasons) is a web-based (accessible via the public internet) system developed by the ITD for the Child Development Bureau to facilitate electronic reporting by child care providers. This application database contains Personally Identifiable Information (PII) of school children and their parents. We found that communication link to the application through the internet is not encrypted[9]. Such unencrypted communication link is open to series of attacks that can compromise not only information transmitted on the link, but also the application data repository and County internal systems to which the application is connected.

Good security practice and relevant information security standards (including HIPAA of 1996, PCI DSS, and NIST SP800-53) require the implementation of appropriate security controls to protect confidentiality and integrity of information during transmission.

Recommendation
CAHSD to work with ITD to enhance the security of the application by employing cryptographic mechanism to protect the communication path between external users and the application server.

[9] Encryption is the process of using mathematical algorithm to transform plain text information into a format unreadable to persons except those possessing the algorithm key

Management Response
CAHSD concurs with this finding and responds to the recommendations as follows:

The application was modified by ITD in September, 2012 to ensure end to end industry standard encryption between external users and the County system to prevent unauthorized access/eavesdropping by anyone except the authorized user when the application is accessed.

Finding 3.
Policies for managing computer users' passwords on department/County computing resources are weak *(Appendix I # T.3).*

We found that department personnel are not required to periodically change the passwords to their domain accounts. The domain account for each employee grants access to department/County computing resources. Good security practice requires that users change their account passwords periodically (e.g. every 90 or 180 days). Failure to change password periodically gives malicious users or attackers almost endless time to figure out user's password, or to continue to use passwords that are already compromised. We found users that had not changed their domain account passwords in more than three (3) years. ITD is responsible for enforcing password policy across County networks.

Also, users of the Enhanced Field System (EFS) used in the Child Development Bureau are neither required to use strong password nor change password periodically. The EFS is owned and mandated by the State of Florida for the School Readiness (SR) and Voluntary Pre-kindergarten (VPK) programs. Core security service to support the system was contracted to Hewlett-Packard (HP) by the state. However, because the state allowed the County to host EFS database and application servers within the County network, the responsibility for managing users' accounts on the EFS application and database was delegated to DHS staff.

Recommendations
a. ITD should enforce password maximum lifetime policy for users' domain accounts.
b. CAHSD should request enhancement to the password policy in the EFS that will require users to use strong passwords and also change them periodically.

Management Response
CAHSD concurs with this finding and responds to the recommendation as follows:

a. Domain Password policies have been developed which are aligned with information security best practices. These requirements were enabled for all CAHSD accounts in a phased implementation to minimize user impact and business interruption. This implementation was completed on September 27, 2012.

b. *EFS database is being replaced by Early Learning Information System (ELIS) throughout the State of Florida. The roll out in Dade County is scheduled for July 2013. The EFS administrator is being trained in the new database which is a more robust and secure application that provides password policy configuration and more secure features*

Finding 4.
Access rights of some former and transferred employees were not removed from the Social Services Information System (SSIS) and the Enhanced Field System (EFS) for months/years after the employees had been separated or transferred *(Appendix I # T.4).*

The SSIS is a management information system utilized to record and share information among County departments and agencies on services provided to individuals and families across the County. The system is accessible via the public internet (web-based) and it contains Personally Identifiable Information (PII) of various programs beneficiaries/recipients across the County. We found an employee that retired on April 29, 2011 whose access and administrative privilege in SSIS was not revoked until the end of December 2011 (eight months after the employee ceased to be a legitimate user of the system).

As of November 2011, access rights of twenty two (22) former employees (retired and/or separated) were not revoked in EFS. Two of the employees retired in 2007; one in 2009; five retired or separated in 2010; and the others in 2011. Also, as of November 2011, access rights of twenty three (23) employees transferred to other County departments were not revoked in EFS. In addition, we found ninety three (93) active user accounts in EFS that were not traceable to either current or former employees of DHS.

Significant risk is associated with the above control weakness. System accounts and access privileges of former or transferred employees that are not revoked promptly can become veritable tools for malicious users to breach sensitive and confidential information.

Recommendations
a. CAHSD should delete system accounts of former and transferred employees stated above in EFS; revoke and subsequently delete accounts in EFS whose owners were unidentified.
b. CAHSD should implement written and well-supervised procedures for granting, modifying, monitoring, documenting, and promptly terminating user access on all systems used by the department.

Management Response
CAHSD concurs with this finding and responds to the recommendation as follows:

a. For auditing and historical purposes user accounts cannot be deleted from the EFS system. However, to disable use, accounts are placed inactive and passwords are changed.
b. CAHSD will expand the implementation of the developed CAHSD Policy and Procedure (P&P), "New Accounts, Transfers and Terminations" which establishes that each user is granted a unique identifier for access through a supervisor approved Central Registration System (CRS) form where only the needed operational account privilege is requested and granted. In addition, CAHSD's Human Resources division is in constant contact with CAHSD's Information Technology Unit to disable any accounts and/or passwords for employees who retired, transferred or terminated from the County.

Finding 5.
Processes for fixing software defects and managing computers security settings failed to provide effective remediation of flaws and vulnerabilities in computer systems *(Appendix I # P.1).*

Computer flaws are either configuration errors or program errors/bugs that expose computer system to possible attacks and unauthorized access. Software vendors release patches[10] periodically to correct known errors or bugs in their software. Timely and effective application of those patches, as soon as they are released, is critical to safeguarding vulnerable computers from the activities of computer hackers who frequently search for such vulnerabilities to exploit.

We scanned twenty-six (26) computers (including servers) in DHS and found twenty (20) different types of program errors that remained unpatched months after the vendors had released patches. Because there are different levels of risk associated with software vulnerabilities, industry best practice is to prioritize the speed with which released patches are applied, such that security patches that are rated 'High' risk are applied first before those with lower risk ratings. The goal should be to apply all relevant security patches promptly before attackers exploit the vulnerabilities. ITD patch management policy and procedures require that all security patches be applied to all applicable systems within the County network within one (1) month following the release of patches.

Of the twenty (20) vulnerabilities we discovered on the scanned computers, fifteen (15) were classified as high risk, four (4) as medium risk, and one (1) as low risk. Risk level is determined based on industry Common Vulnerability Scoring System (CVSS), which considers, among other factors, the likelihood and the impacts of a vulnerability being exploited. The number of months that had elapsed since the release of the relevant patches up to the time of our assessment and the risk levels associated with the unpatched system flaws are shown in *Tables 1* and *2* below:

Table 1: *Age Analysis of Unpatched System Flaws*

Months	Number of Patches	%
3 – 6	11	55%
7 – 12	1	5%
13 – 24	1	5%
Over 24	7	35%

Table 2: *Risk Levels of Unpatched System Flaws*

Risk Level	Number of Flaws	%
High	15	75%
Medium	4	20%
Low	1	5%

From the assessment of the twenty-six (26) sampled computers, we also found forty-six (46) system configurations (settings) that did not conform to recommended best practices necessary to mitigate possible inherent risks.

Computers generally have security settings that can be set to different levels, which in turns determine the degree of protection offered to the computer(s) against exploitation. Misconfigurations of computer systems can open up cracks for malicious users to gain

[10] Programs written by software vendors to correct known bugs or errors in their earlier released software

unauthorized access to systems resources and confidential information. Those security settings identified in our assessment as not conforming to recommended best practices, together with their associated risks are summarized in *Table 3* below.

Table 3: *Risk Levels of System Configuration Flaws*

Risk Level	Number of Settings	%
High	1	2%
Medium	8	17%
Low	37	81%

ITD, in conjunction with DHS staff, is responsible for patch and configuration management on department computer systems. Although ITD had automated the process for applying patches to vulnerable computers, there needs to be regular and timely review and follow up on system patched level, in order to: (1) identify remediation that were unsuccessful, in order to reapply them either manually or via automated system; (2) discover new vulnerabilities that need remediation.

Recommendations

a. ITD should review flaw remediation and system configuration management processes, implement needed enhancements that will assure the effective remediation of systems flaws.
b. ITD should develop system configuration standard that ensures all systems security settings conform to best practices that mitigate possible risks.

Management Response

CAHSD concurs with this finding and responds to the recommendation as follows:

a. ITD employs an automated flaw remediation system to correct known system vulnerabilities. The system was recently upgraded improving automated processes for fixing flaws. The system has also been enhanced to detect and correct additional flaws that were not being addressed by the previous version. It is anticipated that the number of software defects will be significantly reduced. Integrated with the automated fix process, ITD will provide CAHSD regular reports on systems that are non-compliant for follow-up and manual correction of flaws that the automated system cannot fix.

b. CAHSD and ITD will work together to develop a system configuration standard that ensures all systems security settings conform to best practices that mitigate possible risks within the next 90 days.

Finding 6.

There was no policy for secure use of removable storage media, and no documentations to provide evidence of secure sanitization or destruction of old electronic storage media *(Appendix I # P.2a & 2b).*

DHS transfers all computers (including their hard drives) scheduled for donation or disposal to the Property Surplus Division of the Internal Services Department (ISD). Personnel in the Property Surplus Division remove hard drives from computers before donating or disposing the

computer boxes. According to ISD personnel, all hard drives are physically destroyed with a hammer, however there were no documentations to evidence what was destroyed, when it was destroyed, how it was destroyed, and by whom it was destroyed.

We also noted that DHS did not have a policy for the secure use of removable storage media (such as flash drives, DVDs, etc.). Neither the DHS nor the ISD had written policy or guidelines on how to securely sanitize or destroy storage media, and what documentation to maintain as evidence of sanitization or destruction actions. Good security practice demands that organization have functional policy and procedure for the use, sanitization, reuse and disposal of storage media. In addition, there should be sufficient documentation to track media sanitation/disposal actions (i.e. what was disposed, when, how, and by whom).

Without appropriate policy and guidance to ensure secure usage, removable storage media containing confidential information may be used insecurely. Also without written evidence, it is difficult to prove that all media meant for sanitization or destruction were properly sanitized or destroyed.

Recommendation
CAHSD and Internal Service Department, in conjunction with ITD, should establish written policy and guidelines for secure use, sanitization, reuse and destruction of storage media (hard disk and removable media), and documentation requirements to evidence sanitization and destruction actions.

Management Response
CAHSD concurs with this finding and responds to the recommendations as follows:

> *ITD's Field Services Division has in place a Media-Vise compact desktop/laptop hard drive destruction unit. The Media-Vise Compact unit allows safe and quick destruction of data stored on County IT hard drive assets. ITD and CAHSD will be coordinating to leverage our existing SLA with the Field Services Division to establish a disk/data destruction procedure which has led to the destruction of 50 hard drives on October 1, 2012.*

Finding 7.
Policy for secure custody of clients' files/records was violated in two of the DHS sites we visited *(Appendix I # P.3).*

DHS policy on client file security and maintenance requires that all case files/client records be maintained securely in cabinets with locks and keys. For the Child Development Bureau, the policy also requires that retrieved or new files must be returned promptly to the Record Center upon completion of service or no later than the end of each work day.

During a spot check conducted on November 15, 2011 at the CDS Eligibility Office at Miami Gardens, we found that more than twenty four (24) case files retrieved from the Record Center for over 3-10 work days were not returned as of the time of the spot check. We noted, however, that at the counterpart Naranja Neighborhood Office, there was full compliance with this policy.

At the Central Intake Unit of the Rehabilitative Service Bureau, Clients Identifying Data Record forms (for substance abuse clients) slated for shredding were kept in an open box that was stored in the unit Supervisor's office bathroom. Janitorial personnel had unsupervised access to the supervisor's office.

Not keeping case files/records securely, as required, could expose confidential information to unauthorized personnel, which could result to data breaches. According to *Ponemon Institute LLC* report on the *United States 2011 Cost of Data Breach Study*[11], the average cost (direct and indirect expenses to organizations) of data breach per compromised record is $194.

Recommendation

CAHSD Personnel must ensure full compliance with the department's policy on secure custody of client files and records. Records slated for shredding should be given equivalent protection until they are shredded.

Management Response

CAHSD concurs with this finding and responds to the recommendation as follows:

a. *Requires that all Upper Level Management consider protecting MDC office areas that contain information assets, and information processing facilities.*
b. *Require that all CAHSD's employees take part in all County-Wide Security Awareness Training and Refresher. As of September 24, 2012, 89% of employees have completed the Mandatory Security Awareness Refresher Training. We planning to have this mandate completed by October 31, 2012.*
c. *Also, HIPPA online training will be provided agency wide to the staff whose works requires the manipulation of sensitive and confidential clients' data.*
d. *Requested link to CAHSD Policies & Procedures be pushed out to all CAHSD workstations upon final approval of P&P.*

Finding 8.

Department did not have policy or guidelines to ensure that user-developed databases and spreadsheets containing clients confidential information are secured with appropriate security mechanisms *(Appendix I # A.1).*

We found an unsecured Microsoft Access database developed by staff in the Refugee Youth and Family program that contained replicate records from the official State-owned software used for the program. The Access database was developed by staff for in-house backup and reconciliation purposes, and it resided on an employee's desktop computer connected to the internet. The database, which contained confidential information such as social security number, date of birth, maiden name, alien number etc., was not protected with any security features. Storing sensitive and confidential information in unencrypted spreadsheets or databases on computer(s) connected to the internet is not a recommended practice.

[11] http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-us.en-us.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2012Mar_worldwide__CODB_US

Good security practice demands that organization establish effective policy and procedures to ensure that computer systems and databases containing sensitive or confidential information are secured with appropriate security features. This should include both vendor-developed systems and those developed in-house. User-developed databases and applications are particularly susceptible to poor security features when there is no security policy and procedures to ensure appropriate security features are employed to secure such systems.

Good security practice also requires that encryption, truncation or similar mechanisms be used to conceal or disguise sensitive contents in data repository (database). This security feature provides an additional layer of protection for the data in case a person gains unauthorized access to the database.

Recommendations

a. CAHSD, in consultation with ITD, should implement adequate security mechanisms (including encryption) to protect all existing user-developed databases that contain confidential information in the department.
b. CAHSD, in consultation with ITD, should develop written policy and guidelines that will ensure all in-house and user-developed applications and databases are secured with appropriate security mechanisms before they are put to use.

Management Response

CAHSD concurs with this finding and responds to the recommendation as follows:

a. The Department will assess and inventory databases currently in use within the department.
- *Request inventory of databases & spreadsheets for security assessment.*
- *Identify databases & spreadsheets owners and custodians.*
- *Appropriate security measures will be implemented for those databases, including the access to the Secure File Transfer Protocol (SFTP) server.*

b. The In-House Programming Policy and Procedure was developed and waiting for approval and dissemination throughout the entire CAHSD.

Attachment 1

Memorandum

MIAMI-DADE COUNTY

Office of the

OCT 0 5 2012

Commission Auditor

Date: October 1, 2012

To: Charles Anderson, CPA, Commission Auditor
Board of County Commissioners, Office of the Commission Auditor

From: Lucia Davis-Raiford, Executive Director
Community Action and Human Services Department

Subject: Audit of Internal Controls for the Protection of Electronically Stored Personal and Health Information (Former Human Services Department)

We are in receipt of the Final Draft memorandum dated September 4, 2012, on the above referenced subject as issued by the Board of County Commissioners' Office of the Commission Auditor (OCA). This serves to provide Community Action and Human Services Department (CAHSD) and Information Technology Department's (ITD) response to the reported findings and recommendations from that memorandum.

Finding 1 - Department uses wireless local area network (WLAN) implemented with poor security features that can easily compromise confidential and sensitive information.

OCA Recommendations:

a. ITD should upgrade wireless local area network (WLAN) to one based on security standards with robust security features (e.g. Wi-Fi Protected Access II (WPA2).
b. ITD should establish effective risk assessment and control processes to continuously manage the risks of wireless network.

CAHSD Response - CAHSD concurs with this finding and responds to the recommendations as follows:

a. CAHSD requested that ITD's Field Services Division provide an estimate for implementation of wireless security. ITD, working closely with CAHSD completed the estimate as requested. An implementation plan will be created based on the assessment and estimate. Historically, network equipment located at departmental sites was purchased by departments, either as part of the initial deployment or purchased as needed to replace aging, unsupported equipment. Support and maintenance of the original equipment was provided by ITD. The purchase of replacement equipment as part of modernization or upgrade of the network was funded by departments and implemented by ITD. Recently, ITD adopted a new support model whereby aging network equipment is replaced with newer equipment providing additional functionality and security. The purchase, maintenance and recapitalization of the equipment is now included in a monthly "port charge" of $10.00/active port. A port is defined as the point where a network device (computer/server/printer) is connected to the County's network. The annual service charges include deployment, configuration, management and recapitalization/replacement of the network equipment. This updated business model ensures that each participating department's network will remain current, state of the art, supported and secure.
b. ITD will develop an effective risk assessment and control processes to continuously manage the risks of wireless network. This will be completed within 90 days after the wireless security implementation plan is approved. The new equipment being proposed for deployment (and associated port charges) is part of the Edge Network Infrastructure project which will update network infrastructure throughout the County. This project was intended to modernize the County's network as well as improve wired and wireless security to meet current standards and best

practices. This new infrastructure for both wired and wireless connectivity will be managed centrally by ITD and the risk management process will be integrated as part of the overall management of the network. Although CAHSD was not included in the 2012/13 deployment plan, the department and associated sites will be expedited and should be completed by March 2013.

Finding 2 - Communication link between external users and the County internal network for one important application (computer program) used in the Child Development Bureau was not protected with appropriate security mechanisms.

OCA Recommendations:

a. CAHSD to work with ITD to enhance the security of the application by employing cryptographic mechanisms to protect the communication path between external users and the application server. (Used in the Child Development Bureau).

CAHSD Response - CAHSD concurs with this finding and responds to the recommendations as follows:

a. The application was modified by ITD in September, 2012 to ensure end to end industry standard encryption between external users and the County system to prevent unauthorized access/eavesdropping by anyone except the authorized user when the application is accessed.

Finding 3 - Policies and processes for managing computer users' passwords and accounts on department and County computing resources were weak.

OCA Recommendations:

a. ITD should enforce password maximum lifetime policy for users' domain accounts
b. CAHSD should request enhancement to the password policy in the EFS that will require users to use strong passwords and also change them periodically.

CAHSD Response - CAHSD concurs with this finding and responds to the recommendation as follows:

a. Domain Password policies have been developed which are aligned with information security best practices. These requirements were enabled for all CAHSD accounts in a phased implementation to minimize user impact and business interruption. This implementation was completed on September 27, 2012.
b. EFS database is being replaced by Early Learning Information System (ELIS) throughout the State of Florida. The roll out in Dade County is scheduled for July 2013. The EFS administrator is being trained in the new database which is a more robust and secure application that provides password policy configuration and more secure features.

Finding 4 - Access rights of some former and transferred employees were not removed from the Social Services Information System (SSIS) and the Enhanced Field System (EFS) for months/years after the employees had been separated or transferred.

OCA Recommendation:

a. CAHSD should delete system accounts of former and transferred employees stated above in EFS; revoke and subsequently delete accounts in EFS whose owners were unidentified.
b. CAHSD should implement written and well-supervised procedures for granting, modifying, monitoring, documenting, and promptly terminating user access on all systems used by the department.

CAHSD Response - CAHSD concurs with this finding and responds to the recommendation as follows:

a. For auditing and historical purposes user accounts can not be deleted from the EFS system. However, to disable use, accounts are placed inactive and passwords are changed.
b. CAHSD will expand the implementation of the developed CAHSD Policy and Procedure (P&P), "New Accounts, Transfers and Terminations" which establishes that each user is granted a unique identifier for access through a supervisor approved Central Registration System (CRS) form where only the needed operational account privilege is requested and granted. In addition, CAHSD's Human Resources division is in constant contact with CAHSD's Information Technology Unit to disable any accounts and/or passwords for employees who retired, transferred or terminated from the County.

Finding 5 - Processes for fixing software defects and managing computers security settings failed to provide effective remediation of flaws and vulnerabilities in computer systems.

OCA Recommendations:

a. ITD should review flaw remediation and system configuration management processes, implement needed enhancements that will assure the effective remediation of system flaws.
b. ITD should develop system configuration standard that ensures all systems security settings conform to best practices that mitigate possible risks.

CAHSD Response – CAHSD concurs with this finding and responds to the recommendation as follows:

a. ITD employs an automated flaw remediation system to correct known system vulnerabilities. The system was recently upgraded improving automated processes for fixing flaws. The system has also been enhanced to detect and correct additional flaws that were not being addressed by the previous version. It is anticipated that the number of software defects will be significantly reduced. Integrated with the automated fix process, ITD will provide CAHSD regular reports on systems that are non-compliant for follow-up and manual correction of flaws that the automated system cannot fix.
b. CAHSD and ITD will work together to develop a system configuration standard that ensures all systems security settings conform to best practices that mitigate possible risks within the next 90 days.

Finding 6 - There was no policy for secure use of removable storage media, and no documentations to provide evidence of secure sanitization or destruction of old electronic storage media.

OCA Recommendations:

a. CAHSD and Internal Service Department, in conjunction with ITD, should establish written policy and guidelines for secure use, sanitization, reuse and destruction of storage media (hard disk and removable media), and documentation requirements to evidence sanitization and destruction actions.

CAHSD Response - CAHSD concurs with this finding and responds to the recommendations as follows:

a. ITD's Field Services Division has in place a Media-Vise compact desktop/laptop hard drive destruction unit. The Media-Vise Compact unit allows safe and quick destruction of data stored on County IT hard drive assets. ITD and CAHSD will be coordinating to leverage our existing SLA with the Field Services Division to establish a disk/data destruction procedure which has led to the destruction of 50 hard drives on October 1, 2012.

Finding 7 - Policy for secure custody of clients' files/records was violated in two of the DHS sites we visited.

OCA Recommendation:

CAHSD Personnel must ensure full compliance with the department's policy on secure equivalent protection until they are shredded.

CAHSD Response - CAHSD concurs with this finding and responds to the recommendation as follows:

a. Requires that all Upper Level Management consider protecting MDC office areas that contain information assets, and information processing facilities.
b. Require that all CAHSD's employees take part in all County-Wide Security Awareness Training and Refresher. As of September 24, 2012, 89% of employees have completed the Mandatory Security Awareness Refresher Training. We planning to have this mandate completed by October 31, 2012.
c. Also, HIPPA online training will be provided agency wide to the staff whose works requires the manipulation of sensitive and confidential clients' data.
d. Requested link to CAHSD Policies & Procedures be pushed out to all CAHSD workstations upon final approval of P&P.

Finding 8 - Department did not have policy or guidelines to ensure that user-developed databases and spreadsheets containing clients' confidential information are secured with appropriate security mechanisms.

OCA Recommendation:

a. CAHSD, in consultation with ITD, should implement adequate security mechanisms (including encryption) to protect all existing user-developed databases that contain confidential information in the department.

b. CAHSD in consultation with ITD, should develop written policy and guidelines that will ensure all in-house and user-developed application and databases are secured with appropriate security mechanisms before they are put to use.

CAHSD Response - CAHSD concurs with this finding and responds to the recommendation as follows:

a. The Department will assess and inventory databases currently in use within the department.
   - Request inventory of databases & spreadsheets for security assessment.
   - Identify databases & spreadsheets owners and custodians.
   - Appropriate security measures will be implemented for those databases, including the access to the Secure File Transfer Protocol (SFTP) server.

b. The In-House Programming Policy and Procedure was developed and waiting for approval and dissemination throughout the entire CAHSD.

I look forward to your response and to working collaboratively to ensure that the Community Action and Human Services Department continues to deliver excellence and complies with all County regulations.

Should you need additional information/clarification, please do not hesitate to contact Delia Iglesias at (786) 469-4601 or Alberto Parjus at (786) 469-4754).

C: Russell Benford, Deputy Mayor, Office of the Mayor
Alberto Parjus, Assistant Director, CAHSD
Delia A. Iglesias, Supervisor, Information Technology Unit, CAHSD
Angel Petisco, Director, ITD
Lars Schmekel, Chief Security Officer, ITD