



CITY AUDITOR'S OFFICE

Human Services Information Controls

January 14, 2016

AUDIT REPORT NO. 1610

CITY COUNCIL

Mayor W.J. "Jim" Lane
Suzanne Klapp
Virginia Korte
Kathy Littlefield
Linda Milhaven
Guy Phillips
Vice Mayor David N. Smith



January 14, 2016

Honorable Mayor and Members of the City Council:

Enclosed is the audit report for *Human Services Information Controls*, which was included on the Council-approved FY 2015/16 Audit Plan. We reviewed Human Services information controls, particularly security management and information system access, to protect clients' personally identifiable information (PII). The scope of our audit encompassed the Human Services Department's seven operating facilities, including Adaptive Services, the Community Assistance Office, the two community/neighborhood centers, the two senior centers and Youth & Family Services.

Our audit found that comprehensive policies, procedures and records management could better ensure client personally identifiable information is protected. Also, physical storage of PII can be better secured, and information technology management and controls can be strengthened.

We appreciate the cooperation and assistance of the Human Services Department during the course of this audit. If you need additional information or have any questions, please contact me at (480) 312-7867.

Sincerely,

A handwritten signature in blue ink that reads "Sharron Walker".

Sharron E. Walker, CPA, CFE, CLEA
City Auditor

Audit Team:

Cathleen Davis, CIA - Senior Auditor
Dan Spencer, CIA - Senior Auditor

TABLE OF CONTENTS

AUDIT HIGHLIGHTS	1
BACKGROUND	3
Table 1. Examples of PII and Sensitive PII	3
Figure 1. Human Services Department’s Facilities and Programs	5
OBJECTIVES, SCOPE, AND METHODOLOGY	7
FINDINGS AND ANALYSIS	9
1. Comprehensive policies, procedures and records management could better ensure client personally identifiable information (PII) is protected.	9
2. Physical storage of PII can be better secured.	11
Table 2. Areas for Physical Control Improvement	12
3. Information technology management and controls can be strengthened.	13
MANAGEMENT ACTION PLAN	17
APPENDIX	21



AUDIT HIGHLIGHTS

Human Services Information Controls

January 14, 2016

Audit Report No. 1610

WHY WE DID THIS AUDIT

This audit was included on the Council-approved FY 2015/16 Audit Plan to review Human Services information controls, particularly security management and information system access, to protect clients' personally identifiable information (PII).

BACKGROUND

The Human Services Department manages federal, state, local and private resources to provide safe and sanitary housing, social services, economic growth, self-sufficiency, reasonable accommodations for persons with disabilities or low to moderate income, and senior programs. Part of the Community Services Division, the Department operates 7 facilities.

To participate in most of the Department's programs, individuals must provide varying types and amounts of PII.

PII is defined as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

City Auditor's Office

City Auditor 480 312-7867
Integrity Line 480 312-8348
www.ScottsdaleAZ.gov

WHAT WE FOUND

- 1. Comprehensive policies, procedures and records management could better ensure client PII is protected.**
We found that while Department staff collects sensitive PII from their clients, City and Department policies and procedures do not currently provide staff with sufficient guidance on protecting the information. Further, a coordinated records management program could help reinforce PII protection.
- 2. Physical storage of PII can be better secured.**
Improvement can be made in the Department's physical controls over areas where PII is stored, including:
 - Access controls to facilities and client files
 - Issuance and control of keys
 - Protection of network assets
- 3. Information technology management and controls can be strengthened.**
User access to the Department's systems and shared network folders are not needs-based. In addition, system implementation can be more effectively managed.

WHAT WE RECOMMEND

We recommend the Human Services Department:

1. Ensure comprehensive policies and procedures are developed for securing PII collected, used, stored, shared and disposed. Also, require staff to evaluate PII to ensure only necessary information is being collected and that collected information is protected. Develop a training and awareness program for all staff with access to PII. Finally, designate a records coordinator to assist each area with records management, including records inventories and dispositions.
2. Develop policies and procedures and employee training to appropriately address its physical security controls.
3. With the assistance of Community Services technology staff, develop written guidance for granting and reviewing system access and obtain security group detail for use in evaluating user access rights. Also, limit access to network folders containing PII and ensure future system implementations are timely and documentation is maintained.

MANAGEMENT RESPONSE

The Department agreed with the audit recommendations and expects to have all recommendations implemented by January 2017.

BACKGROUND

According to the City's fiscal year (FY) 2015/16 Operating Budget, the Human Services Department manages federal, state, local and private resources to provide safe and sanitary housing, social services, economic growth, self-sufficiency, reasonable accommodations for persons with disabilities or low to moderate income, and senior programs. As part of the Community Services Division, the Department operates 7 facilities with a \$14 million budget, which consists of \$4 million from general funds plus an additional \$10 million from grants and special programs, and 64.9 full-time equivalent employees. In addition, the Department estimated it has the assistance of 550 to 600 volunteers per year.

To participate in most of the Department's programs, individuals must provide varying types and amounts of personal information. National standards exist that define and provide guidance on protecting this personally identifiable information.

The National Institute of Standards and Technology (NIST) *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* defines PII as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

Unauthorized access, use or disclosure of PII can seriously harm both individuals, by contributing to identity theft, blackmail or embarrassment, and the organization, by reducing public trust in the organization or creating legal liability.

NIST Guide

Some PII is more sensitive and requires stricter handling guidelines as it could substantially harm an individual if lost, compromised or disclosed without authorization. Table 1 illustrates the difference between PII and sensitive PII.

Table 1. Examples of PII and Sensitive PII

PII	Sensitive PII
Name	Social Security Number
Home Address	Driver's License Number
Phone Number	Financial Account Number
Email	Biometric Identifiers

SOURCE: U.S. Department of Homeland Security *Handbook for Safeguarding Sensitive Personally Identifiable Information*

In addition, although the Human Services Department is not a covered entity, the Health Insurance Portability and Accountability Act (HIPAA) provides guidance that can be referred to for best practice in protecting health information. HIPAA defines protected health information (PHI) as any information held by a covered entity which relates to health status, provision of healthcare, or payment for health care that can be linked to an individual. Further, the HIPAA Security Rule establishes criteria for protecting electronic PHI, including administrative, physical and technical safeguards.

The Human Service program application processes and forms vary among the different areas, from paper-based forms that may be filled out with the assistance of a City representative to electronic forms that can be filled out and submitted online or via email. Figure 1, on page 5, summarizes the Department's program areas.

Most Human Service programs maintain their service records in paper format at the individual facilities. Therefore, for program services that are provided at multiple facilities, such as food assistance, staff found it difficult to determine frequency of assistance provided to the same individuals. Several years ago to help manage the potential for duplicate services, Community Services staff developed an Access database that was shared by Paiute Neighborhood Center and Vista del Camino Community Center staff.

To improve customer service, performance management tracking and service delivery and to replace the Access database, the Department procured a vendor-supported cloud-based system in October 2014. Because the Client Assistance Management System, or CAMS, is cloud-based, it allows authorized users to access client service records from any location, whether in the office or at a client's home, using an internet-connected device. However, the transition from recordkeeping that is primarily paper-based to the CAMS is still on-going. All Human Services areas except Adaptive Services were instructed to use the system starting October 1, 2015.

Figure 1. Human Services Department's Facilities and Programs

	Adaptive Services Provides services and programs designed to meet the expressed needs of Scottsdale residents with disabilities, to enhance quality of life and promote optimal leisure functioning and inclusive recreation participation.
	Community Assistance Office Administers Community Development Block Grant (CDBG) and HOME Program funds to provide decent housing, suitable living environments and/or expand economic opportunities, primarily for low and moderate income persons.
	Granite Reef Senior Center Provides health & wellness, recreation & fitness and social services including case management, information & referral, and home visit assessments.
	Paiute Neighborhood Center Provides social services for Scottsdale residents including translation, notary, emergency food boxes, bus passes, information & referral and seasonal holiday programs.
	Via Linda Senior Center Provides health & wellness, recreation & fitness and social services including case management, information & referral, and home visit assessments.
	Vista del Camino Community Center Provides social services for Scottsdale residents to prevent homelessness, meet basic needs of individuals and families in crisis and assist individuals to maintain self-sufficiency.
	Youth & Family Services Provides restorative services for juveniles; outreach services for families seeking parenting, conflict, substance abuse, behavioral health and juvenile law help; and educational workshops.

SOURCE: Auditor analysis of the Department's webpages on www.scottsdaleaz.gov.

OBJECTIVES, SCOPE, AND METHODOLOGY

An audit of Human Services Information Controls was included on the City Council-approved fiscal year (FY) 2015/16 Audit Plan. The audit objective was to review Human Services information controls, particularly security management and information system access, to protect clients' personally identifiable information (PII).

To gain an understanding of Human Services PII and related controls, we interviewed Human Services and Community Services management and information system support personnel.

We reviewed related audit reports issued by this office, including *Concerned Citizens for Community Health Contract Compliance* - Audit Report No. 1208 issued in June 2012 and *Compliance with Medical Privacy Requirements of the Federal Health Insurance Portability and Accountability Act (HIPAA)* - Audit Report No. 1010 issued in April 2010. In addition, we reviewed related audit reports recently completed by other auditors.

To gain an understanding of requirements, guidelines and best practices, we reviewed the following:

- U.S. Department of Commerce National Institute of Standards and Technology *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010.
- U.S. Department of Homeland Security *Handbook for Safeguarding Sensitive Personally Identifiable Information*, March 2012.
- Related federal laws including the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act (HIPAA).
- Relevant sections of the Arizona Revised Statutes, including §§ 41-4172 and 44-7601.
- Related Administrative Regulations (AR) including AR 100 *Access to City Facilities*, AR 136 *Network and Computer Security* and AR 295 *Citywide Records Management Program*.
- Related policies and procedures provided by the Community Assistance Office, Paiute Neighborhood Center and Vista del Camino Community Center. Adaptive Services, the Granite Reef Senior Center, the Via Linda Senior Center and Youth & Family Services did not have written PII-related policies and procedures.

To evaluate the effectiveness of controls designed to protect clients' personally identifiable information, we:

- Observed public and staff areas at various Human Services locations and attempted to access areas containing PII, such as file cabinets, file rooms and staff offices.
- Reviewed Facilities Management's records related to the Department's key assignment and Municipal Security's records related to the Department's key card access.
- On a judgmental basis, reviewed a sample of paper client files in each of the Human Services Department locations.

- Evaluated user access to the Department's shared electronic resources containing PII in relation to general job responsibilities.
- Reviewed the CAMS request for proposal, contract and implementation documentation in relation to PII access and security controls.
- Evaluated the Department's information system access controls including written procedures, user security group assignment and password requirements.
- Reviewed available records related to PII training and awareness.

Our audit found that comprehensive policies, procedures and records management could better ensure client personally identifiable information is protected. Also, physical storage of PII can be better secured and information technology management and controls can be strengthened.

We conducted this audit in accordance with generally accepted government auditing standards as required by Article III, Scottsdale Revised Code §2-117 et seq. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Audit work took place from October 2015 to December 2015.

FINDINGS AND ANALYSIS

1. Comprehensive policies, procedures and records management could better ensure client personally identifiable information (PII) is protected.

While the Human Services Department staff collects sensitive personally identifiable information (PII) from their clients, City and Department policies and procedures do not currently provide staff with sufficient guidance on protecting the information. Further, a coordinated records management program could help reinforce PII protection.

- A. The Human Services staff collects client PII for a variety of purposes, such as eligibility determination or service identification. As well, in some instances, certain medical information is collected to facilitate care in the event that issues arise during program participation. Currently, comprehensive PII policies and procedures are not available either at the citywide or department level to guide staff in protecting and securing this information as it is collected, used, stored, shared and disposed.

One authoritative source, the *NIST Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (NIST Guide), states that “organizations should develop comprehensive policies and procedures for handling PII at the organization level, the program or component level, and where appropriate, at the system level.” The NIST Guide further states that organizations should consider developing privacy policies and associated procedures for:

- Access to PII within a system
- PII retention schedules and procedures
- PII incident response and data breach notification
- Privacy during information system development phases
- Limitations on collection, disclosure, sharing, and use of PII
- Consequences for failure to follow privacy requirements

While three of the seven service areas have some written PII guidance, these policies and procedures are generally limited to file storage, file security and volunteer confidentiality requirements. Strong policies and procedures protecting PII reduce possible reputation and legal risks and help to ensure individual privacy is protected.

- B. At times, the Department’s programs appear to collect some unnecessary personal information, such as copies of birth certificates, driver’s licenses and other sensitive documents and data. Human Services has not assessed whether all PII currently being collected by the various service areas is necessary for determining program eligibility, providing services or other specific reason.

A very effective way to minimize the risk of exposing sensitive PII is to not collect it unless necessary. In fact, the City’s Records Management Manual notes that divisions should not collect unnecessary information, especially personal information. Further, the Manual states that to comply with the provisions of A.R.S. §§ 41-4172 and 44-7601, all divisions and offices must:

1. Review the records they maintain on a regular basis to identify personal information.
2. Establish written procedures to identify records containing personal information and protect that information from unauthorized access.
3. Annually, review and update procedures concerning the collection of identifying information to verify whether the information collected is essential to the records being created or received.

Although some Department staff indicated they reviewed records on a regular basis, the reviews were not documented.

As an example of best practice, when requesting PII, federal agencies are required to disclose the authority for requesting the information and whether providing the information is mandatory or voluntary.¹ Also, a comprehensive privacy statement covering the types of personally identifiable information collected, why it is collected and relevant disclosures and security measures would help to assure clients of the care taken when collecting and protecting their personally identifiable information.

- C. The Department can lessen PII risks by providing ongoing awareness efforts and training for staff with access to PII. The NIST Guide defines awareness as efforts designed to change behavior or reinforce desired PII practices and the goal of training to build knowledge and skills that will enable staff to protect PII. Further, the organization should have a training plan and leadership should communicate to staff the seriousness of protecting PII.

The Department's awareness efforts could include a confidentiality agreement for staff with access to PII. Almost 100 Human Services employees have access to client files containing sensitive PII. Providing a written statement of the need to protect PII and maintain its confidentiality for staff to sign in acknowledgement could serve as an annual reminder.

- D. The Human Services Department can improve its records management. Only one area has designated a records coordinator, which assigns responsibility for becoming familiar with the City's Records Management program requirements.
 1. Of the seven Human Services areas, only the Community Assistance Office has its records listed on the Community Services Records Inventory and Essential Records listings. Yet all of the service areas have relevant records, including intake/assessment forms, program applications, consent forms, sign-in sheets, authorizations, evaluations, and surveys. Besides meeting the records management requirements, maintaining a records inventory and an essential records listing would aid the service areas in evaluating their records for proper handling of PII.
 2. The City's Records Management Program also has requirements related to record dispositions. Specifically, records are to be disposed of once the retention period has been reached and the records coordinator is to document their destruction on a Certificate of Records Destruction and file it with the City Records Manager.

¹ The Federal Privacy Act of 1974 requires that, to protect the privacy and rights of individuals, federal agencies must state "the authority (whether granted by statute, or by Executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary" when requesting information.

Although Human Services records have been disposed of by City staff or through a third-party vendor during the past four years, Certificates of Records Destruction have not consistently been prepared and provided to the City Clerk's office. The most recent certificates on file at the City Clerk's office were for Community Assistance Office records destroyed in October 2013. Other Human Services areas have not filed certificates since February 2012.

Having designated records coordinators in the separate service areas can help ensure that the Department's records are appropriately maintained, retained, and preserved or disposed.

Recommendations:

Human Services Department management should:

- A. Ensure comprehensive policies and procedures are developed for securing PII collected, used, stored, shared and disposed.
- B. Require Human Services staff to evaluate the personally identifiable information being collected to ensure that only necessary information is collected and that collected information is protected. Further, consider developing a Human Services privacy statement along with relevant disclosures and security measures.
- C. Develop a program to provide awareness of PII protection requirements, an annual confidentiality statement and periodic training for all staff with access to PII.
- D. Ensure each Human Services area designates a records coordinator to assist with records management. Then require the records coordinators to:
 1. Include all relevant Human Services records on the Records Inventory and Essential Records lists.
 2. Dispose of records in accordance with the established retention period, and document the destruction on a Certificate of Records Destruction to be filed with the City Clerk's Office.

2. Physical storage of PII can be better secured.

Physical controls include the methods used to control access to buildings and offices as well as the cabinets or other storage where files containing PII are located. We observed the physical controls being used at each of the seven Human Services Department facilities. Table 2 on page 12 summarizes areas where physical access controls can be improved to better protect PII.

(Continued on next page)

Table 2. Areas for Physical Control Improvement

	Adaptive Services	CAO	Granite Reef	Paiute	Via Linda	Vista del Camino	Youth & Family Services
Door Access ¹	x		x	x	x	x	x
Key Issuance and Control ²		x	x	x	x		x
IT Network Access ³	x			x	x		
Paper File Access ⁴	x		x	x	x		x
Printer/Copier/Fax/Shredder Access ⁵			x	x		x	

An “x” indicates the location’s physical controls over PII can be improved.

¹ Control: Doors leading to areas containing PII are secured when not in use or monitored as appropriate. Some interior and/or exterior doors were found unattended and/or unsecured.

² Control: Regular door and file cabinet key inventory and assignment reviews are performed. Door key analysis completed for the co-located Community Assistance Office and Paiute Neighborhood Center. File cabinet key analysis completed at each location.

³ Control: Network assets are protected in secured areas with adequate ventilation and cooling. Some network assets were found unsecured, primarily due to ventilation issues.

⁴ Control: Client files containing PII and/or sensitive PII are secured or attended. Some client files containing PII or sensitive PII were found unsecured.

⁵ Control: Client files containing PII and/or sensitive PII are secured or attended. Some documents containing sensitive PII were found unsecured on or near a printer/copier, shredder and/or fax machine.

SOURCE: Auditor observation and analysis of Human Services Department facilities.

General categories for improvement included:

- Access controls to facilities, such as ensuring all exterior and interior doors leading to rooms where PII is stored are secured; staff-only areas where PII is printed, copied, faxed or shredded are segregated and access monitored; and public access to certain facility areas is monitored.
 - ✓ Some staff offices where PII was stored were left unattended and unlocked at times. Due to the nature of the Department’s services, the public, other City staff and volunteers are often in the staff office areas.
 - ✓ Unlocked file cabinets were maintained in public areas (such as near a reception area or in a conference room) at some facilities. Also, the file cabinets maintained in staff areas were not always locked when unattended.

- ✓ PII was found unattended near printer/copiers and fax machines at some facilities. Further, at one facility, a document containing a name and address was found on top of the shredder.

- Protection of network assets, such as network components being secured in dedicated rooms and provided adequate cooling.

At many of the Department's facilities, network assets were maintained in easily accessible unlocked areas. At one facility, the network assets were in an open supply closet. Department staff stated that the door to the supply closet had to remain open for computer ventilation purposes.

- Issuance and control of door keys, including a regular inventory and assignment review.

Due to the amount of time involved to obtain the reports, we reviewed key assignments for two of the seven Human Services facilities. At one facility, 36 keys had been issued for the main building; 11 keys are listed as lost and 3 as stolen. Further, 2 keys for this building were issued to a third-party that operates in a separate building at the facility and 5 were issued to City staff not based at the facility.

- Issuance and control of file cabinet keys, including regular key inventory and assignment review.

At one facility, numerous door and file cabinet keys were found unattended in an unlocked, vacant office. At another facility, the file cabinet keys were kept in an unlocked drawer of a nearby desk located in an open office area.

Specific observations were communicated to Department staff and management, but are not detailed in this report due to their sensitive nature.

Recommendation:

Human Services Department management should develop policies and procedures and employee training to appropriately address its physical security controls.

3. Information technology management and controls can be strengthened.

Information technology (IT) controls are important to prevent unauthorized access to systems and data, and particularly for PII protection. To achieve this control, user access to the Department's systems and shared network folders must be needs-based. In addition, system implementation can be more effectively managed.

- A. User authorization to the Human Services Client Assistance Management System (CAMS) and other systems can be improved by formalizing access approvals, documenting user group rights, and ensuring user access is based on the "least privilege" principle.

1. If properly implemented, the Human Services Client Assistance Management System (CAMS) has the potential to better protect PII than the current paper-based records. However, access to the new CAMS and other Department systems has been granted based on verbal requests and without defined requirements to evaluate whether the requested access is appropriate.

As of November 2015, Human Services had granted 25 staff "Case Worker" access and 11 staff "Intake" access to CAMS. According to the Community Services Technology Coordinator, a written description of these standard security groups' access rights was not available, so Department management assigned staff based on his understanding gained through verbal discussion with the vendor. As of December 2015, the Community Services technology group has not received written documentation of the standard security groups' access rights, including to which system activities each group has read-only, create, modify and/or delete access. Ensuring appropriate system access reduces the risk of exposure or misuse of client data, including sensitive PII. Further, since users can access the cloud-based CAMS from any internet-connected device without being in the office and on the City's network, this control is even more important.

2. Currently, the Department does not grant system access rights based on the least privilege principle.
 - Human Services staff with CAMS access can access all client information as the access is not restricted to relevant program areas. For instance, if added to CAMS, sensitive PII related to the Youth & Family Services juvenile diversion program and medical information collected for the Adaptive Services programs would be available to any staff granted CAMS access. Sensitive information should be limited to only those with a business need for access.
 - CAMS access rights are not revoked timely or reviewed. Two former Human Services staff still had access to CAMS as of November 2015 even though they separated from City employment in October 2015. Upon notification, the Technology Coordinator removed these two users' access.
 - Six of the ten staff with access to the Community Assistance Office's Section 8-related system have been given System Administrator rights. Given the power of System Administrator rights, this type of access should be limited to as few staff as possible.

Applying the principle of "least privilege" access serves to assign user access rights based on the least access needed to successfully complete day-to-day job duties.

- B. Access to the Department's shared network folders and files, many of which contain PII, could be better controlled.

As of December 2015, approximately 90 City staff had access to the Department's various shared network folders. Excluding IT support staff, it appeared that only about 60% of the authorized staff needed access to a given Department folder for their day-to-day job duties. For example, 17 staff in the Parks & Recreation Department, working at locations such as Chaparral and Eldorado Parks, have access to these shared network folders. Six other City staff in areas such as Fire & Life Safety Services and Facilities Management also have access. Additionally, certain files containing PII that Human Services staff thought were password-protected were not.

- C. Although not the focus of this audit, we noted that CAMS implementation was untimely and key phases were not documented.

The Department purchased CAMS in October 2014 and subsequently paid annual subscription and software license fees totaling about \$25,000 for November 2014 to October 2015. However, Human Services staff did not actually start using CAMS until

October 1, 2015. Human Services management indicated that staff was busy with holiday programs, such as the Adopt-a-Family and Adopt-a-Senior programs, and then the Community Services technology staff was diverted to another software implementation project within the division. Due to these delays, Human Services staff training for CAMS began in July 2015 and operational use started on October 1, 2015. Therefore, about \$18,750 in subscription fees and software lease license fees were paid to the vendor during the period when the software was not being used in the Department's operations.

In addition to the untimely implementation, the Community Services technology staff did not maintain documentation of the implementation plan and related correspondence with the vendor, Department communication, testing plans and results, and City acceptance of the system's successful implementation. Further, existing data was not migrated to the CAMS; therefore, users will have to continue referencing older systems and paper files until a useful client history accumulates in the new system.

Recommendations:

Human Services management should ensure that the Department:

- A. With the assistance of Community Services technology staff:
 1. Develops written guidance for granting and reviewing user system access, including maintaining records of the user access approvals and regular access reviews.
 2. Obtains security group access details from the CAMS vendor and reviews the user access rights to ensure appropriate segregation of duties and access based on the least privilege principle. Further, the Department should request staff access to CAMS be removed immediately upon their separation from the City or transfer to another department, and ensure the number of System Administrators for all Department systems is reduced to the minimum number feasible.
- B. Ensures access to network folders containing PII is limited to staff with a business need to access the information for their day-to-day job duties.
- C. For any future system implementations, timely implements systems to ensure the City does not pay subscription and licensing fees for software that is not being used. Further, ensure technology staff develops a written implementation plan and documents related correspondence with the vendor, system testing results, system acceptance and other necessary system implementation activities.

MANAGEMENT ACTION PLAN

1. Comprehensive policies, procedures and records management could better ensure client personally identifiable information (PII) is protected.

Recommendations:

Human Services Department management should:

- A. Ensure comprehensive policies and procedures are developed for securing PII collected, used, stored, shared and disposed.
- B. Require Human Services staff to evaluate the personally identifiable information being collected to ensure that only necessary information is collected and that collected information is protected. Further, consider developing a Human Services privacy statement along with relevant disclosures and security measures.
- C. Develop a program to provide awareness of PII protection requirements, an annual confidentiality statement and periodic training for all staff with access to PII.
- D. Ensure each Human Services area designates a records coordinator to assist with records management. Then require the records coordinators to:
 1. Include all relevant Human Services records on the Records Inventory and Essential Records lists.
 2. Dispose of records in accordance with the established retention period, and document the destruction on a Certificate of Records Destruction to be filed with the City Clerk's Office.

MANAGEMENT RESPONSE: Agree

PROPOSED RESOLUTION: After meeting with City Audit staff, each of the Human Services Managers has agreed to develop and implement for their areas comprehensive policies and procedures for collecting, using, storing, sharing and disposing of PII. This plan will include the following:

- Staff will evaluate PII to include collecting only necessary information in each HS Center.
- Staff will develop a confidentiality statement which will be signed by employees as part of every annual review process.
- The Human Services Training team will develop an educational plan to include awareness of PII protection requirements, confidentiality statements for all staff with PII access.
- A records coordinator will be designated in each HS area and they will maintain Records Inventory and Essential Records lists.
- Each HS area will dispose of records per established retention periods and file a Certificate of Records Destruction form with the City Clerk's Office.
- Managers will create and monitor key logs and Hirsh passes with each staff transition.

RESPONSIBLE PARTY: Human Services Director, Managers and Coordinators

COMPLETED BY: 1/13/2017

2. Physical storage of PII can be better secured.

Recommendation:

Human Services Department management should develop policies and procedures and employee training to appropriately address its physical security controls.

MANAGEMENT RESPONSE: Agree

PROPOSED RESOLUTION: Reference the Human Services PII comprehensive policies, procedures and educational plan outlined in Item #1 above.

RESPONSIBLE PARTY: Human Services Director, Managers and Coordinators

COMPLETED BY: 1/13/2017

3. Information technology management and controls can be strengthened.

Recommendations:

Human Services management should ensure that the Department:

- A. With the assistance of Community Services technology staff:
 - 1. Develops written guidance for granting and reviewing user system access, including maintaining records of the user access approvals and regular access reviews.
 - 2. Obtains security group access details from the CAMS vendor and reviews the user access rights to ensure appropriate segregation of duties and access based on the least privilege principle. Further, the Department should request staff access to CAMS be removed immediately upon their separation from the City or transfer to another department, and ensure the number of System Administrators for all Department systems is reduced to the minimum number feasible.
- B. Ensures access to network folders containing PII is limited to staff with a business need to access the information for their day-to-day job duties.
- C. For any future system implementations, timely implements systems to ensure the City does not pay subscription and licensing fees for software that is not being used. Further, ensure technology staff develops a written implementation plan and documents related correspondence with the vendor, system testing results, system acceptance and other necessary system implementation activities.

MANAGEMENT RESPONSE: Agree

PROPOSED RESOLUTION: The Human Services Department will coordinate with Kathy Schoepe and Kasey Moyers in the City's Community Services IT Department to develop the following technology management and controls plan:

- Develop written instruction guide to address user system access privileges, including maintaining records for user access approvals.
- Human Services Department and the Community Services IT staff will coordinate with CAMS data base vendor to delineate security access procedures to ensure that appropriate access is based on the least privilege principle. Managers will take immediate action when employee turnovers occur, endeavoring to maintain a minimum number of employees with access to CAMS based on business need to access of PII.
- Human Services Director will coordinate with Community Services IT staff to improve timely use of CAMS and to develop written implementation plan to include vendor participation, system reporting results, and other vital system implementation activities.

Human Services Director and Management will monitor and modify V-drive permissions for each Center related to employee's access related to job duties.

RESPONSIBLE PARTY: Human Services Director, Managers and Coordinators

COMPLETED BY: 1/13/2017

APPENDIX

Summary of Key Recommendations from the *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*²

Key Recommendations

Organizations should:

- Identify all PII they collect and store, including name, personal identification number, address (such as street or email), personal characteristics (such as photograph, fingerprints, biometrics), and information that is linked or linkable to one of these (such as date of birth, race, religion, medical or financial information).
- Minimize the use, collection and retention of PII to what is strictly necessary to accomplish their business purpose and mission.
- Categorize the PII by confidentiality impact (low, moderate or high), which indicates the potential harm that could result if the PII were inappropriately accessed, used or disclosed. Example factors include such considerations as identifiability, sensitivity, and access to/location of PII.
- Apply the appropriate safeguards based on the PII confidentiality impact level.

The NIST-recommended safeguards include operational safeguards, privacy safeguards and security controls.

Operational Safeguards

Policies and procedures and awareness, training and education can help to make certain that individuals are held accountable for implementing safeguards to protect the confidentiality of PII and that these safeguards are functioning as intended.

Policies and Procedures

Develop comprehensive policies and procedures for protecting PII confidentiality at the organization level, the program or component level and, where appropriate, at the system level. Organizations should consider developing privacy policies and associated procedures for the following topics:

- Access to PII within a system
- PII retention schedules and procedures
- PII incident response and data breach notification
- Privacy during information system development phases
- Limitations on collection, disclosure, sharing, and use of PII
- Consequences for failure to follow privacy requirements

² *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, Recommendations of the National Institute of Standards and Technology (NIST), Special Publication 800-122, U.S. Department of Commerce, April 2010.

Further, PII should also be addressed in the organization's incident response policies and procedures to detect incidents rapidly, minimize loss and destruction, identify weaknesses, and restore IT operations rapidly.

Awareness, Training and Education

Designed to change behavior or reinforce desired PII practices, the purpose of *awareness* is to focus attention on the protection of PII. The goal of *training* is to build knowledge and skills that will enable staff to protect PII. To reduce the possibility that PII will be accessed, used, or disclosed inappropriately, all individuals that have been granted access to PII should receive appropriate training. Depending on the roles and functions, important topics may include:

- The definition of PII
- Applicable privacy laws, regulations, and policies
- Restrictions on data collection, storage, and use of PII
- Roles and responsibilities for using and protecting PII
- Appropriate retention and disposal of PII
- Sanctions for misuse of PII
- Roles and responsibilities in responding to PII-related incidents and reporting

Education develops a common body of knowledge that reflects all of the various specialties and aspects of PII protection. It is used to develop privacy specialists who can implement privacy programs within the organization.

Privacy-Specific Safeguards

Usually not needed for other types of data, these controls serve to protect the confidentiality of PII.

Minimizing the Use, Collection and Retention of PII

The practice of minimizing the use, collection and retention of PII is a basic privacy principle. Limiting PII collection to the least amount necessary to conduct the organization's mission may limit potential negative consequences in the event of a data breach involving PII. This general concept is often abbreviated as the "minimum necessary" principle.

An organization should regularly review its previously collected PII to determine whether it is still relevant and necessary. Effective management and prompt disposal of PII, in accordance with approved records retention schedules, will minimize the risk of unauthorized disclosure.

Privacy Impact Assessments

Privacy impact assessments (PIA) are structured processes for identifying and mitigating privacy risks, including risks to confidentiality, within an information system. Some areas that may be addressed include:

- What information is to be collected
- Why the information is being collected
- How the information is intended to be used

- With whom the information will be shared
- How the information will be secured
- What choices the organization made regarding an IT system or information collection as a result of performing the PIA.

The Guide also discusses *de-identifying* and *anonymizing* information as additional privacy-specific safeguards. Both remove enough PII that an individual cannot be identified in the remaining data. However, the de-identifying safeguard retains a separate reference table for re-identifying the information, while the anonymizing safeguard does not.

Security Controls

Following are examples of information security controls that help safeguard the confidentiality of PII.

- *Access Enforcement* - Using access control policies and access enforcement mechanisms help safeguard PII. One example is implementing role-based access control configured so that each user can access only the pieces of data necessary for the user's role.
- *Separation of Duties* - Enforcing separation of duties that involve access to PII.
- *Least Privilege* - Enforce the most restrictive set of access rights and privileges needed by users to perform their specified tasks. For example, ensure that users who need access to records containing PII only have access to the minimum amount of PII and only those privileges (e.g., read only, write) that are necessary to perform their job duties.
- *Remote Access* - Prohibiting or strictly limiting remote access to PII.
- *Transmission Confidentiality* - Protecting the confidentiality of transmitted PII by encrypting communications or the information before transmission.

City Auditor's Office

7447 E. Indian School Rd., Suite 205
Scottsdale, Arizona 85251

OFFICE (480) 312-7756
INTEGRITY LINE (480) 312-8348

www.ScottsdaleAZ.gov/auditor

Audit Committee

Councilwoman Suzanne Klapp, Chair
Councilmember Virginia Korte
Councilwoman Kathy Littlefield

City Auditor's Office

Kyla Anderson, Senior Auditor
Lai Cluff, Senior Auditor
Cathleen Davis, Senior Auditor
Brad Hubert, Internal Auditor
Dan Spencer, Senior Auditor
Sharron Walker, City Auditor



The City Auditor's Office conducts audits to promote operational efficiency, effectiveness, accountability, and integrity.