



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.