Human Services Department
Privacy Controls – Information Mgmt Plans
December 12, 2018

Report Highlights

Information Management Plans
The Human Services Department created information management plans in accordance with City policies and IT standards. However, the plans did not account for all personal identifying information collected, and did not address oversight of authorized third parties.

Personal Identifying Information
Logical and physical controls to protect personal identifying information are in place; however, Human Services should strengthen controls by establishing a Department-wide policy and by improving controls over hardcopy papers.
Executive Summary

Purpose

We evaluated the Human Services Department (HSD) compliance with City privacy-related policies, and with City Information Technology (IT) standards, including the development and implementation of Information Management Plans (IMPs).

Background

Maintaining information privacy and protection is essential to preserving the City’s public trust. Through multiple Administrative Regulations (ARs) and City IT standards, the City has defined policies to protect personal identifying information (PII) and restricted City information (RCI). These policy statements are outlined in Attachment A, City Privacy-Related Policies. In general, these policy statements require departments to create information management plans that detail where PII is collected, and how it is secured. These policies also require that: (1) appropriate contract language be used when PII is collected by or shared with vendors, (2) staff be properly trained in privacy-related policies, and (3) appropriate safeguards over PII are in place.

HSD staff deal primarily with PII in their job functions, and only with RCI on a limited basis. PII is in hardcopy format (primarily applications, case notes, and application forms) as well as electronic format (case notes, emails, and documents). This electronic data is saved in HSD’s Case Management System (CMS).

Results in Brief

**HSD developed IMPs in accordance with City policies and IT standards, using the City’s template. However, some IMPs did not account for all PII collected, and some did not address oversight of authorized third parties, through verification of appropriate data security systems and procedures.**

HSD developed IMPs for all necessary groups, but in some instances those IMPs did not reflect all PII that is collected, or all entities with which the PII is shared. The IMPs also listed sufficient controls and protective measures, except for ensuring that third parties collecting or storing PII on the City’s behalf have appropriate controls as outlined in A.R 1.91 Data Shared with Third-Parties.

**In general, logical and physical access to electronically-stored PII was adequately controlled. However, access to paper PII was not adequately controlled.**

In general, HSD safeguarded PII in CMS by employing appropriate user account and password management controls. These controls can be strengthened by maintaining documentation of user account approval, and by periodically reviewing account permissions. Physical access to PII requires strengthening; management practices regarding badge access, key inventory logs, and key physical security, are not implemented consistently. These controls can be strengthened by assigning unique
access codes to staff until badge readers can be installed, using key inventory logs, and securing all physical keys.
## Department Responses to Recommendations

### Rec. #: 1.1 Review and amend (at the earliest time reasonable) contracts that do not have the required data privacy contract language as outlined in A.R 1.91 Information Privacy and Protection Supplement – Data Shared with Third Parties.

**Response:** The department will identify and amend all contracts requiring the change.  
**Target Date:** December 31, 2019

**Explanation, Target Date > 90 Days:** Amending the contracts takes time as it involves third parties. Contracts will be reviewed for amendment as part of the regular amendment schedule throughout a year.

### Rec. #: 1.2 Update the HSD Information Management policies and procedures to include:

- A record review process that aligns with each division’s record retention schedule
- Identification of the designated Security Liaison
- Language that requires all employees to complete the required security awareness training and any additional training required by contractual or federal funding agreements (i.e., Department of Economic Security Awareness Training)
- An annual review process to update the information management policy
- The use of encrypted email when sending confidential information outside the City as outlined in City IT Standards 1.12 Handling Confidential Information
- An annual process to ensure employees are aware of and agree with required policies and procedures

**Response:**

- IMP’s will be updated to document the annual review and purge process that is currently conducted.
- IMP’s will identify the assigned Security Liaison
- HSD adheres to the city mandated training that is implemented by ITS. IMP’s will be updated to reflect this compliance.
- An annual review of the IMP is currently conducted and reported back to ITS as required. Moving forward a review date will be added to the document.
- Staff will continue to be informed of the IMP changes as IMP updates occur.

**Target Date:** January 30, 2019

**Explanation, Target Date > 90 Days:** N/A

### Rec. #: 1.3 Work with Information Technology Services (ITS) and the Information Security and Privacy Office (ISPO) to implement a procedure to monitor and verify that third parties have appropriate data security systems in place as agreed upon in executed contracts.
**Response:** All HSD contracts require contractors to implement appropriate controls to safeguard the data we provide. Also, contractors are liable for any damages due to a data breach. Due to the operational and legal complexities involved, the department will request ISPO, Procurement, and Law to provide guidance in ensuring that sensitive data is protected at all times.

**Target Date:** January 30, 2019

**Explanation, Target Date > 90 Days:** N/A

**Rec. #:** 2.1 In compliance with City IT Standard s1.3 – Identity Management, formalize and document the CMS account provisioning process. Ensure the process includes the documenting of access requests and approvals, the disabling and suspending of accounts, and the review of access rights at least annually.

**Response:** A form for requesting CMS access will be created. New users will be able to login only after the business owner has approved the request. Program staff will review accounts annually and make changes as necessary.

**Target Date:** January 30, 2019

**Explanation, Target Date > 90 Days:** N/A

**Rec. #:** 2.2 Use the City’s standard building key issue form to log and track keys issued.

**Response:** The form will be rolled out to all locations and staff trained on implementation and usage.

**Target Date:** January 30, 2019

**Explanation, Target Date > 90 Days:** N/A

**Rec. #:** 2.3 Education Services – Until badge access readers are installed, assign unique access codes to Head Start staff and any others who have a business need to access the work area.

**Response:** Unique access codes will be assigned to Head Start staff who have a business need.

**Target Date:** January 30, 2019

**Explanation, Target Date > 90 Days:** N/A

**Rec. #:** 2.4 Education Services – Ensure all physical keys are stored securely.

**Response:** Key’s will be stored in a key locker with an identified chain of custody in accordance with AR 4.44.

**Target Date:** January 30, 2019

**Explanation, Target Date > 90 Days:** N/A
1 – Compliance with City Privacy Policies

Background

Multiple City Administrative Regulations (ARs), and IT standards, guide departments in handling and protecting PII and RCI. Attachment A, City Privacy-Related Policies, summarizes these guidelines.

To assess HSD’s compliance, we reviewed applicable privacy policies and standards, HSD IMPs, and supporting documentation. We also observed the physical and electronic storage of data.

Results

HSD has an established information management privacy program with completed IMPs for the Department’s various divisions. The program can be improved by ensuring all data is included in the IMPs and Department policies are updated to reflect current procedures.

We evaluated compliance with each of the ARs and City IT privacy standards outlined in Attachment A (see page 8).

- Media Retention and Removal (City IT Standard s1.7) – HSD uses the Case Management System (CMS) application to store and manage its electronic records. HSD actively evaluates which records have met the record retention statute, and removes records that have met that criteria. We confirmed that the last record purge was conducted on March 24, 2018.

- Records Management Program (A.R. 1.61) – HSD is aware of the records management program; however, physical records are not consistently reviewed and archived based on the Department record retention schedule.

- Information Security Management (A.R. 1.84) – HSD has appointed a Department Information Security Liaison with appropriate authority to serve as the Department’s liaison. However, when meeting with the different divisions, not everyone was aware of who the Information Security Liaison was.

- Information Privacy & Protection (A.R. 1.90) – HSD has created a Department-specific information management policy; however, we noted the policy has not been reviewed since 2015 and needs to be updated to reflect newly adopted Department processes, procedures, and training. We verified that staff has completed the required City of Phoenix Security Awareness Training. We also verified that additional training, such as the Department of Economic Security Training, was completed by the required divisions.

- Data Shared with Third-Parties (A.R. 1.91) – Not all contracts with HSD vendors contained the required data privacy contract language. We reviewed 12 contracts and found that nine contained the required language. In addition, most IMPs did not address the oversight of authorized third parties through verification
of appropriate data security systems and procedures. Divisions stated they were unsure of how to comply with this requirement.

- City Privacy Program (A.R. 1.95) – We found that HSD’s IMPs did not account for all PII that is gathered, stored, and removed. PII such as Social Security Numbers or other government identification numbers, gender, age, or race were not accounted for on certain IMPs. In addition, the IMPs did not account for all third-parties that PII is shared with, both inside and outside the City.

- Contract Worker Background Screening (A.R. 4.45) – This will be reviewed in another audit that will focus on the contract worker background screening process, Background Checks (#1190021).

- Information Management Plans (City IT Standard b1.4) – HSD created IMPs for divisions who collected, processed, accessed, stored, disclosed, and destroyed PII and RCI. No exceptions noted.

Recommendations

1.1 Review and amend (at the earliest time reasonable) contracts that do not have the required data privacy contract language as outlined in A.R 1.91 Information Privacy and Protection Supplement – Data Shared with Third Parties.

1.2 Update the HSD Information Management policies and procedures to include:
   - A record review process that aligns with each division’s record retention schedule
   - Identification of the designated Security Liaison
   - Language that requires all employees to complete the required security awareness training and any additional training required by contractual or federal funding agreements (i.e., Department of Economic Security Awareness Training)
   - An annual review process to update the information management policy
   - The use of encrypted email when sending confidential information outside the City as outlined in City IT Standard s1.12 Handling Confidential Information
   - An annual process to ensure employees are aware of and agree with required policies and procedures

1.3 Work with Information Technology Services (ITS) and the Information Security and Privacy Office (ISPO) to implement a procedure to monitor and verify that third parties have appropriate data security systems in place as agreed upon in executed contracts.
2 – Assessment of Information Management Plans

Background

*City IT Standard b.1.4 – Information Management Plan* provides guidance to departments completing their IMPs, and standardizes the IMP template that is to be used by all departments. The City’s standardized IMP template consists of multiple choice questions that are generated via an online survey. IMPs are used to document the privacy-related PII and RCI that a department collects, uses, stores, and/or shares with another department or business entity.

We validated controls for IMPs regarding the handling and transmitting of PII to ensure those processes comply with *City IT Standard s1.12 – Handling Confidential Information*. PII and RCI are stored in the Case Management System (CMS).

Results

*Established user account management controls are in place for CMS; however, controls can be improved through regular reviews of access rights.*

The CMS system uses role-based user groups to provide access to individual user accounts. Each division is responsible for entering users into CMS. HSD does not use a physical user access request form to document account provisioning and define access rights in CMS. Rather, HSD relies on Active Directory controls, new hire documentation, and supervisors’ judgement to determine account provisioning and access rights. Access to CMS is configured to disable user access after 60 days of inactivity. Access is also restricted when the Active Directory account is disabled. Outside of the initial account setup, reviews of access rights are not conducted. Per *City IT Standard s1.3 – Identity Management*, all access is to be requested by the supervisor and approved by the business owner. Such documented approval (either hardcopy or via a system such as Remedyforce) is to be maintained for the life of the account. Additionally, access rights are to be reviewed at least annually to ensure they remain appropriate over time as staff’s roles and duties change.

*CMS authentication controls comply with City IT Standard s1.5 Password Management.*

CMS is a single sign-on application configured to authenticate with Active Directory. Using Active Directory for authentication ensures that password requirements comply with City standards. No exceptions were found.

*Physical access to PII is not sufficiently restricted at all sites.*

We reviewed five sites that store PII. The data collected includes Social Security Numbers, dates of birth, and other sensitive information. We reviewed controls over access by badges, and access by keys (including keys to file cabinets, desk drawers, etc.).
## PII and RCI Physical Controls for HSD Sites

<table>
<thead>
<tr>
<th>Site</th>
<th>Badge Access Controls</th>
<th>Records in Locked Cabinet</th>
<th>Records in Locked Room</th>
</tr>
</thead>
<tbody>
<tr>
<td>Family Advocacy Center</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Travis Williams Family Center</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Adam Diaz Senior Center</td>
<td>N/A</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>McDowell Place Senior Center</td>
<td>N/A</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>South Mountain Senior Center</td>
<td>N/A</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

Controls are in place at HSD sites; however, controls require strengthening to prevent inappropriate access to PII and RCI.

Exceptions noted:

- Travis Williams Family Service Center – Education Services staff use a shared office access code to enter their work area within the facility, thereby eliminating the ability to trace access to specific individuals. Additionally, the file cabinet key is maintained in a common area and accessible to those without a business need to access those files.

- McDowell Place Senior Center – The key inventory log does not capture staff signatures to document receipt of key(s).

- South Mountain Senior Center – PII is maintained in locking desk drawers; however, there is no inventory tracking of those desk keys.

## Recommendations

2.1 In compliance with *City IT Standard s1.3 – Identity Management*, formalize and document the CMS account provisioning process. Ensure the process includes the documenting of access requests and approvals, the disabling and suspending of accounts, and the review of access rights at least annually.

2.2 Use the City’s standard building key issue form to log and track keys issued.

2.3 Education Services – Until badge access readers are installed, assign unique access codes to Head Start staff and any others who have a business need to access the work area.

2.4 Education Services – Ensure all physical keys are stored securely.
Attachment A – City Privacy-Related Policies

A.R. 1.84 – *Information Security Management*
Defines the City’s Information Security Management Program which provides the framework to protect the confidentiality, integrity, and availability of information captured, stored, maintained, and used by the City. Requires department heads to appoint a Department Information Security Liaison with appropriate authority to serve as the department’s liaison for compliance with information security requirements.

A.R. 1.90 – *Information Privacy & Protection*
Establishes Citywide policies to protect personal identifying information (PII) and restricted City information (RCI) regardless of the format, and applies to all employees, contractors, and third parties. The A.R. defines PII, RCI, breach, and critical breach. In addition, the A.R. specifies that PII and RCI: should only be accessed in order to perform specific job-related duties, should be secured and protected at all times to avoid unauthorized access, and should be redacted and destroyed through appropriate secure methods. The A.R. also requires departments to develop an Information Management Plan (IMP), establish and outline departmental policies for the creation, access, use, and destruction of PII and RCI, and to ensure all affected employees, business partners, and third parties are aware of and trained on the department’s IMP and the A.R at least annually.

A.R. 1.91 – *Information Privacy & Protection Supplement – Data Shared with 3rd Parties*
Provides guidance to City departments when sharing data, including PII and RCI, with a third party. The A.R. requires departments to provide oversight to third parties who have access to the department’s data, including PII and RCI. Prior to sharing data with a third party, the department must:

- Document in the IMP why sharing PII and RCI with third parties is necessary.
- Clarify in the IMP the data being shared that is considered PII and/or RCI.
- Require the third party to comply with state, federal, and local privacy laws, and City policies.
- Verify whether the third-party conducts background checks of its employees and any other individuals who will have access to PII and RCI.
- Verify whether the third party has appropriate data security systems and procedures.
- Require the third party to acknowledge that it is prohibited from releasing information to other independent parties and from using the information for any purpose other than that for which it received the information.
- Require the third party to notify the contracting department immediately if a breach is suspected.
• Require the third party to acknowledge that it is prohibited from notifying individuals affected by a breach or critical breach of the City’s information without prior written consent of the City.
• Include provisions in written contracts with third parties that require data security safeguards.

A.R. 1.95 – Privacy Program
Establishes the City’s privacy program. The A.R. defines the City’s privacy principles, and establishes roles, responsibility, and authority of the City’s Chief Privacy Officer (CPO), the Information Security & Privacy Office (ISPO), the Information Privacy Oversight Council, and the Information Security & Privacy Liaison.

City IT Standard b1.4 – Information Management Plan
Defines what an Information Plan is and requirements regarding how frequently the plans are to be updated, to whom they are submitted, and submission deadlines.
Scope, Methods, and Standards

Scope

We evaluated PII and RCI collected by HSD and its contractors while completing City business. We also evaluated controls over the collection and storage of this information. We compared these practices to Information Management Plans (IMPs) submitted in May 2018. We conducted our testing in August and September 2018.

Methods

We evaluated compliance with City privacy policies by reviewing procedures, practices, and IMPs related to the collection, transmission, and storage of PII and RCI. We gained a basic understanding of the current process by reviewing all six IMPs submitted to the Information Security & Privacy Office (ISPO). We conducted a risk assessment to narrow our testing of controls to those IMPs deemed to be the most critical. Based on this risk assessment, we reviewed the Case Management System and the PII collected from vulnerable populations.

In conducting fieldwork, we met with primary contacts responsible for each IMP to review the accuracy and adequacy of plans. These plans detail what PII and RCI data items are kept, with whom they are shared, and the controls safeguarding the data. We then tested the controls by physical observation for hard copy data, or by a system review for electronic data. We also reviewed contracts of entities with whom PII or RCI is shared.

Unless otherwise stated in the report, all sampling in this audit was conducted using a judgmental methodology to maximize efficiency based on auditor knowledge of the population being tested. As such, sample results cannot be extrapolated to the entire population and are limited to a discussion of only those items reviewed.

Standards

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the performance 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.