Recommendations

4

Follow-up Report

Personal Information Data Privacy

(Internal Audit report #22/23-2 issued February 2023)

The Office of County Internal Audit:
Elizabeth Pape, CIA, CFE – County Internal Auditor
Aaron Kay – Performance Auditor

Audit committee:
Daryl Parrish, Chair - Public member
Jodi Burch – Public member
Joe Healy - Public member
Kristin Toney – Public member
Summer Sears – Public member
Stan Turel - Public member
Patti Adair, County Commissioner
Charles Fadeley, Justice of the Peace
Lee Randall, Facilities Director

To request this information in an alternate format, please call (541) 330-4674 or send email to internal.audit@Deschutes.org

Table of Contents:

1. Introduction

Audit Authority

The Deschutes County Audit Committee has suggested that follow-ups occur within nine months of the report. The Audit Committee would like to make sure departments satisfactorily address recommendations.

Background on Department and Original Audit

This initial assessment of personal information data privacy was to demonstrate a commitment to and thoughtful protection of personal information. Personal information is data that distinguishes an individual, such as full legal name, driver's license, or social security number. Additional risk comes with additional pieces of personal data. Generally, one piece of personal information alone cannot be used to steal a person's identity. It's the various pieces put together that risks compromise of an individual's identity.

Overall, the County demonstrated a strong grasp of data privacy handling and only a couple of areas resulted in recommendations. Staff in departments/offices handling personal information exceed 99% of County staff. The County's departments/offices that deal with HIPAA or law enforcement were unilaterally found to have greater awareness and procedures.

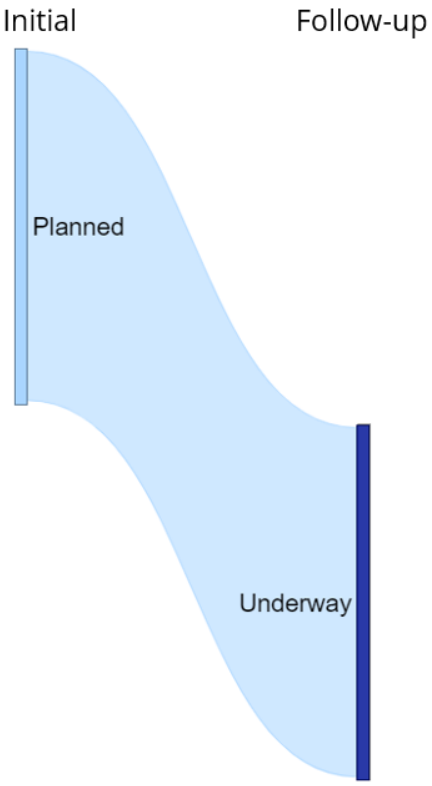
The audit identified the following areas for further improvement, including:

- additional administrative safeguards could help with personal information awareness;
- department/office utilization of technology with personal information could be strengthened;
- some departments/offices retain or collect personal information they do not need; and
- county policy does not reflect update to statute.

2. Follow-up Results

The follow-up included four outstanding recommendations agreed to by multiple County departments and offices. **Figure I** provides an overview of the resolution status of the recommendations. The details of the follow-up are included at the end of the report in **Appendix A**. In interpreting the status, Internal Audit may sometimes raise or lower the status provided by the department based on communication received from the department.

Figure I – How were recommendations resolved?



With this follow-up, none of the outstanding recommendations have been fully addressed. This outcome is not wholly unexpected, given the breadth of the recommendations spanning the entirety of County operations. Many County departments/offices have reported completing portions of the four recommendations, but until an updated policy is approved and a countywide program including a risk assessment process have been established, the status will be considered underway.

3. Appendix A: Updated workplan (status as of December 2023)

Recommendation	Status	Estimated Resolution	Updated Comment
It is recommended for the County departments/offices to assign an employee over each department's/office's personal information security program who will also be responsible for establishing appropriate training and compliance with County policy.	**Underway**	September-24	**Admin-** After GA-9 is updated and resources are identified, County Administration will begin coordinating with Department Heads to implement this recommendation. **IT-** The IT department has assigned an employee who is responsible for ensuring that the data that IT collects for our business processes is compliant with regulations and training is provided to the IT department. Data that is stored on behalf of departments/offices within IT infrastructure and systems is the responsibility of the respective department/offices. **911-** Our Administrative Manager/Technical Manager will jointly be responsible for this task. We maintain secure records with locking cabinets/offices, and our computers are locked when someone is not at their desk. Our technical and physical safeguards are managed. Between both our Administrative and Technical Manager they can identify internal/external risks and train employees as required in policy GA-9. If training is a requirement county-wide it would be great to have a universal training for employees. Outside of our locked personnel files we do not house store any PHI information elsewhere. Additionally, staff must be certified biannually in information security best practices as a requirement to access CJIS and LEDS. If/when the policy is updated we will review and make necessary adjustments pertaining to the policy.

Recommendation	Status	Estimated Resolution	Updated Comment
It is recommended for departments/offices to consider the risks and develop and/or deploy technology appropriate to the situation for communicating and sharing personal information.	**Underway**	June-24	**Admin-** County Administration is currently working with IT to identify tools and resources to assist departments with implementation. **IT-** We have successfully partnered with many departments on safeguards related to transferring personal information via Secure File Transfer Protocol (FTP) and have created documented processes that can be shared and adapted for use by other teams. What has not been created or communicated is where not to share PII data. Today, the County's shared drive is secure at the business unit level. IT is currently responsibly for defining security permissions for the department's top level shared drive based on HR's input to IT which includes people who have been hired or terminated. IT recommends that the departments maintain this level of security and perform auditing, if needed. Departments can work with IT to develop reporting so that managers can periodically monitor permissions of shared drives. **911-** After discussion with amongst our Leadership Team it was determined that we do not have the need to send encrypted emails since we do not send PHI or other confidential information via email. However, we did train all the admin staff on how to turn encryption on in their email if we deem it necessary. In a circumstance where there is a question on if it needs to be turned on the employee will reach out to County Legal for direction. **Finance-** Completed. Staff training occurred in February 2023 and access to files and servers was verified with IT to

Recommendation	Status	Estimated Resolution	Updated Comment
			limited Finance personnel or those with necessary business needs.
It is recommended County departments/offices consider whether they are following policies and could reduce the amount of personal information they collect or retain and make changes to associated processes.	**Underway**	June-24	**Admin-** County Administration is currently working with IT to identify tools and resources to assist departments with implementation. **IT-** We agree with this recommendation and can support departments/offices with finding technical solutions, if necessary.
It is recommended the County update policy GA-9 to reflect the substantive changes from the revised Oregon Consumer Information Protection Act.	**Underway**	February-24	**Admin-** County Administration is currently updating GA-9.

4. Appendix B: Objective, Scope, and Methodology

Objective and Scope

"Audit objectives" define the goals of the audit.

Objective:

The objective was to follow up on recommendations from the original audit.

Scope and timing:

The follow-up included four recommendations from the internal audit report for Personal Information Data Privacy #22/23-2 issued in February 2023. The original internal audit report should be referenced for the full text of the recommendations and associated discussion. The follow-up reflects the status as of December 2023.

Methodology

The follow-up report was developed from information provided by Whitney Hale, Deputy County Administrator, Tania Mahood, County Information Technology Director, Robert Tintle, County Chief Financial Officer, and Sara Crosswhite, 9-1-1 Director. Follow-ups are, by nature, subjective. In determining the status of recommendations that were followed up, we relied on assertions provided by those involved and did not attempt to independently verify those assertions. The updates received were included in **Appendix A**.

Since no substantive audit work was performed, Government Auditing Standards issued by the Comptroller General of the United States were not followed.

If you would like to receive future reports and information from Internal Audit or know someone else who might like to receive our updates, sign up at http://bit.ly/DCInternalAudit.