

**MULTNOMAH COUNTY, OREGON
ADMINISTRATIVE PROCEDURE PII-1**

SUBJECT: Collecting, Safeguarding and Disposing of Personally Identifiable Information

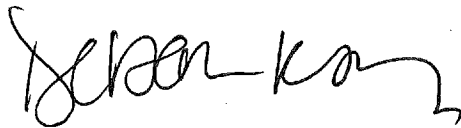
PURPOSE: The purpose of this county-wide administrative procedure is to define Workforce Member responsibilities and procedures for the collecting, safeguarding and disposing of Personally Identifiable Information. It is important that individuals who the County serves have fundamental protection of their personally identifiable information, in compliance with applicable laws, no matter which department collects, maintains or disposes of it.

PROCEDURE

OWNERS (ROLES) County Privacy Officer and County Security Officer

LAST REVISED DATE: February 4, 2020

APPROVED BY:



DEPARTMENTS

AFFECTED: All Departments working with Personally Identifiable Information

LEGAL CITATION/

REFERENCES: Oregon Consumer Information Protection Act ORS 646A.600 et. seq.; Health Insurance Portability and Accountability Act ("HIPAA")

SCOPE: Personally Identifiable Information of individuals covered by this procedure includes that of prospective, current and former clients, residents, consumers, patrons, employees, interns, contractors, volunteers and others with whom the County has or had a relationship.

- I. **Definitions.** See County Administrative Procedure PII-0.
- II. **Collecting Personally Identifiable Information**
 - A. Workforce Members shall collect only the PII required and necessary for the purpose of the business conducted. Workforce Members must not collect PII that is not needed.

B. Workforce Members shall ensure that PII of multiple individuals is never combined into a single record intended to include information of only one individual.

i. When collecting and assigning PII to a County record, verify an individual's identity by collecting unique identifiers. The type and number of unique identifiers will vary depending on the purpose and need for the County record.

ii. Workforce Members shall consult their department/division specific requirements for identity verification.

III. **Safeguarding Personally Identifiable Information**

A. All Workforce Members are responsible for safeguarding and protecting the PII accessible to them to perform their job duties.

i. PII must not be accessed, shared, distributed, used or disclosed except as permitted or required by a Workforce Member's job duties.

1. All Workforce Members that collect PII must follow all safeguards implemented by their department/division consistent with this procedure to ensure that PII is not intentionally or inadvertently made available to the public or disclosed to unauthorized Workforce Members in any way.

2. Before disclosing PII, Workforce Members must verify the identity and authority of the requestor.

a. To verify identity, collect unique identifiers from the individual. The type and number of unique identifiers will vary depending on the request. Workforce Members shall consult their department/division specific requirements for identity verification.

b. If an individual or entity requests PII of a third party, a Workforce Member must verify the authority of that individual or entity to access the requested PII before the PII is disclosed. Authority can be demonstrated by:

i. A public records request and approved response with PII redacted when required (see County Administrative Procedure REC-2),

ii. A law that permits or requires the disclosure,

- iii. Department/division policy/procedure that permits or requires the disclosure, or
 - iv. Valid authorization/release of information.
 - ii. All Workforce Members in possession of PII must appropriately retain and archive any records containing PII in accordance with County retention rules and State laws.
- B. Special Rule for Social Security Number Protection
 - i. Prohibition on Printing and Posting
 - 1. No Workforce Member shall print an individual's full Social Security number on any information that will be sent through the mail (e.g. United States Postal Service) or securely emailed without a written request from the individual, except as required or permitted by law.
 - 2. No Workforce Member shall print an individual's Social Security number on any card required for the individual to access services provided by the County.
 - 3. No Workforce Member shall publicly post or display information containing a full 9-digit Social Security number.
 - ii. Limitations on Disclosure
 - 1. Workforce Members will not provide copies of information containing a full Social Security number of an individual to anyone other than the individual whose Social Security number is listed, except as permitted or required by law.
 - 2. Workforce Members may provide information to a third party with the Social Security number redacted if the information is otherwise allowed to be released to the third party, as described in subsection III.A.
 - iii. This subsection III.B does not prevent the collection, use, or release of a Social Security number as required by state or federal law, or the use or printing of a Social Security number for internal verification or administrative purposes. However, whenever possible, Workforce Members should use only the last four (4) digits of a Social Security number of an individual for verification purposes unless there is a documented compelling business reason to use the full 9-digit Social Security number.
- C. Special Rule for Credit Card/Debit Card Protection

- i. Workforce Members shall not store or display more than the last five (5) digits of a credit card number or debit card number in any system or on any documentation.

D. Transporting Personally Identifiable Information

- i. Workforce Members shall not remove or transport any PII, regardless of form, from County offices, unless such PII is required for the performance of their job duties offsite and approved by a supervisor/manager (if approval required by department/division policy/procedure).
- ii. Workforce Members shall only remove or transport the minimum PII necessary to perform their job duties.
- iii. PII must be under the control of the Workforce Member when removed or transported outside of the office and shall not be left unattended or unsecured (e.g. in a vehicle).

E. Special Rules for Specific Formats

i. Paper Format

- 1. PII in paper format must be stored out of general view when unattended, and must be locked or put away in file cabinets as physical space allows when not in use.
- 2. PII temporarily placed in open containers or boxes located under desks, near trash receptacles or near general recycling containers is not appropriately safeguarded.

ii. Verbal Format

- 1. Verbal discussions of PII in areas where the public is allowed shall be conducted in such a way as to minimize the risk of others overhearing PII. When appropriate, verbal discussions involving PII in areas where the public is allowed should be conducted in enclosed offices, conference rooms, or other private areas.
- 2. Nothing in this procedure prohibits discussion of PII in a Workforce Member's designated workspace, including a cube environment.

iii. Electronic Format

- 1. County owned mobile devices used in conjunction with PII must be registered with IT County mobile device

management. PII must not be stored or downloaded on non-county equipment or devices.

2. Workforce Members must not send electronic transmissions, e.g. emails, containing PII unless permitted for a business purpose or by law.
3. Electronic transmissions, e.g. emails, containing PII sent to an external party must be encrypted. Emails shall be encrypted using the County's secure email service or similar service, such as in response to an encrypted email received from a third party.
4. Workforce Members must lock their computer workstation when leaving it unattended.
5. Sharing PII with other Workforce Members using networked drives, workstations, systems, and mobile devices must be done in accordance with privacy laws and County rules. Questions should be raised to data owner of the system.
6. Secure Print/Walk Up Printing
 - a. Using the secure print function on printing devices reduces the risk of compromise and loss to printed PII and is also a sustainable business practice to reduce wasted paper and reduce cost.
 - b. Workforce Members shall only print PII when a paper version of the PII is required.
 - c. Workforce Members shall use secure print on all printing devices with such capability.

IV. Disposing of Personally Identifiable Information

A. Workforce Members must securely dispose of PII when it is no longer needed for records retention requirements or other business/legal purposes.

- i. Disposing of PII includes removing, disposing or transferring physical storage containing PII.

B. Special Rules for Specific Formats

i. Paper Format

1. Workforce Members must directly dispose of PII in secure/locked shred bins as soon as possible when the information is no longer needed. Each container or box with

PII must be emptied into a secure/locked shred bin by the end of each work day. Under no circumstance may PII be maintained in a container or box overnight. Departments/offices without secure/locked shred bins should send materials to Records Management for secure shredding in accordance with REC -3.

2. Shredding devices for paper are not permitted without approval of the County Chief Operating Officer and by Information Technology Security Manager (IT). Such devices must comply with standards set under NIST Special Publication 800-88 (Guidelines for Media Sanitization) so there is reasonable assurance that the PII cannot be read or reconstructed.

ii. Electronic Format

1. Shredding devices for electronic media are not permitted without approval of the County Chief Operating Officer and Information Technology (IT) Security Manager.
2. Departments/offices without an approved shredding device shall send Removable Electronic Media to Records Management for retention evaluation and/or secure destruction [see County Administrative Procedure REC-3]. Certificates of Destruction shall be retained per the County Records Department as a permanent record per OAR 166-150-0125(10)(a).
3. Departments shall send Fixed Electronic Media for secure disposal/destruction to IT Security. Fixed Electronic Media with PII transferred for disposal/destruction must be secured by IT Security until received by a third party vendor. Access to Fixed Electronic Media transferred in error must be obtained from the IT Security Manager.
4. Workforce Members of the Multnomah County Sheriff's Office and District Attorneys Office must follow their department-specific procedures for disposal of electronic media.

C. Access to Secure/Locked Shred Bins (Paper/Printed Format)

- i. To maintain the security of PII, keys to secure/locked shred bins that contain paper shall not be distributed to Workforce Members.
 - 1. Workforce Members shall not request or hold keys from the vendor that performs shredding services for the County.
 - 2. Vendors shall report any request made to the County Contract Administrator.
- ii. Once PII in paper format is disposed of in a secure/locked shred bin, it may not be retrieved except in very limited circumstances determined on a case-by-case basis as described below.
 - 1. A Workforce Member that has discarded PII in error and would like to retrieve it from a secure/locked shred bin must submit a request via Commons or to privacy@multco.us with the following information:
 - a. Describe the PII that was disposed in error (e.g. what it looks like, type of information it contains).
 - b. Provide the estimated time it would take to recreate or re-request the PII disposed of in error if it cannot be retrieved. Include any relevant factors such as impact on client or County resident.
 - c. Provide the timeframe for the next scheduled pick up by the vendor (if known).
 - 2. Workforce Members must not attempt to retrieve the PII disposed of in error or break/cut the lock on the shred bin.
 - 3. The County Privacy Officer or designee has sole discretion to open a secure/locked shred bin.

V. Monitoring Responsibilities

- A. All Workforce Members are responsible for monitoring for compliance with this procedure.
- B. County supervisors and managers are responsible for reducing their department's risk of exposure for loss or inappropriate disclosure of PII.

VI. Reporting and Notification Procedure

- A. Workforce Members must immediately report a known or suspected event involving the failure of safeguards for or improper disposal of PII required under this procedure.
 - i. Reports can be submitted through
 - 1. The County's Good Government Hotline

2. Department/Division Privacy Contact

3. County Privacy Officer

- ii. Security events (e.g. a lost or stolen mobile device or laptop containing PII) must be reported to the IT Helpdesk at 503-988-4357.

B. Breach Response

- i. The procedure to notify individuals affected by a breach or unpermitted disclosure of PII not subject to HIPAA is covered in County Administrative Procedure PII-2.
- ii. The procedure to notify individuals affected by a breach or unpermitted disclosure of PHI subject to HIPAA is covered in County Administrative Procedure HIPAA-4.

VII. Non-Compliance. Employees who fail to comply with the requirements of this procedure may be subject to discipline.

VIII. Cross-Reference

- A. *Notification Requirements for Unauthorized Acquisition of PII* [PII-2]
- B. *PII Definitions* [PII-0]
- C. *Reporting and Handling of Complaints, Incidents and Breaches of Protected Health Information (PHI)* [HIPAA-4]
- D. County Records Retention Schedules
- E. *Public Records Request* [IT-2]
- F. *Multnomah County Public Records Disclosure Practice* [REC-2]
- G. *Transferring records to the Records Center* [REC-3]
- H. *Use of Information Technology* [County Personnel Rule 3-35]