ADMINISTRATIVE POLICIES

SECTION: 500-Health, Safety and Security	**POLICY#:** 506
TITLE: Personal Information Protection Policy	**R & O** #: 20-79
	IMPLEMENTED BY PROCEDURE #:
SPONSORING DEPT/DIV: Support Services/Information Technology	
ADOPTED: 06/23/2020	**REVIEWED:**

PURPOSE: The purpose of this policy is to address Staff responsibilities regarding the safeguarding of Personal Information. Staff responsibilities under the Health Insurance Portability and Accountability Act (HIPAA) are separate from this policy and are addressed under the County HIPAA Privacy Policy (Policy 501) and the County HIPAA Reporting and Handling of Complaints, Incidents and Breaches of Protected Health Information (PHI) Policy.

APPLICABILITY: This policy and related implementing procedures apply to all elected public officials, employees, volunteers, interns and contractors of Washington County (referred to collectively herein as 'Staff').

AUTHORITY: This policy implements the requirements of the Oregon Consumer Information Protection Act (ORS 646A.600 through 646A.628).

DEFINITIONS: The following are terms commonly referenced in this Policy. In the event of conflict or absence of a term, the definitions set forth in ORS 646A.600 through 646A.628 shall govern:

Breach of Security:

1. "Breach of Security" means an unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of Personal Information that a person maintains or possesses.
2. "Breach of Security" does not include an inadvertent acquisition of Personal Information by a person or the person's employee or agent if the personal information is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality or integrity of the Personal Information.

3. "Data Security Officer" means an individual designated by department director to be the subject matter expert on this policy and related procedures.

Personal Information:

1. Written or electronic information including a person's first name or first initial and last name in combination with any one or more of the following data elements, if encryption, redaction or other methods have not rendered the data elements unusable or if the data elements are encrypted and the encryption key has been acquired:
    a. Social Security number;
    b. Driver's license number or state identification card number issued by the Oregon Department of Transportation;
    c. Passport number or other identification number issued by the United States;
    d. Financial account number, credit or debit card number in combination with any required security code, access code or password that would permit access to a person's financial account or any other information or combination of information that a person reasonably knows or should know would permit access to the person's financial account;
    e. Data from automatic measurements of a consumer's physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate the consumer's identify in the course of a financial transaction or other transaction;
    f. Health insurance policy number or health insurance subscriber identification number in combination with any other unique identifier that a health insurer uses to identify the consumer; or
    g. Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer.

2. A username or other means of identifying a consumer for the purpose of permitting access to the consumer's account, together with any other method necessary to authenticate the username or means of identification.

3. Any of the data elements or any combination of the data elements described in paragraphs 1 or 2 above without the consumer's username, or the consumer's first name and first initial and last name, if:
    a. Encryption, redaction or other methods have not rendered the data element or combination of data elements unusable; and
    b. The data element or combination of data elements would enable a person to commit identity theft against a person.

4. "Personal Information" does not include information in a federal, state or local government record, other than a Social Security number, that is lawfully made available to the public.

Staff:

1. All individuals performing services for the County including, elected public officials, employees, volunteers, interns and contractors.

GENERAL POLICY: All Staff have a responsibility to safeguard Personal Information in their care and to report a Breach of Security. This policy provides guidance on how to protect and maintain files and devices that contain Personal Information.

POLICY GUIDELINES:

1. Responsibilities:

    a. Collecting Personal Information
        i. Staff must only collect the Personal Information required and necessary for the purpose of the business conducted. Staff should not collect Personal Information that is not needed.
        ii. When collecting and assigning Personal Information to a County record, Staff must 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.
        iii. Staff is responsible to ensure that Personal Information of multiple individuals is not combined into a single record inadvertently.

    b. Maintaining Personal Information

    Staff whose work involves maintaining Personal Information are responsible for protecting the confidentiality, integrity and availability of the Personal Information. Departments shall maintain business procedures specific to their areas for managing Personal Information. These procedures should be stored in a central repository, accessible by Staff in their respective areas.

    c. Protection of Social Security Numbers (SSN)

    Staff shall not print an individual's full SSN on any document that will be sent through the mail without a written request from the individual whose SSN will be printed on the document or as required or permitted by law. Staff will only use the last four digits of an SSN on all documents unless there is a documented and

compelling business or legal reason to use the entire SSN. If a document contains a full SSN, Staff must take steps to protect the document from unauthorized disclosure. Staff will not provide copies of a document containing a full SSN to anyone other than the individual whose SSN is listed on the document, except as allowed by state or federal law. Staff may provide a copy of a document to a third party with the SSN redacted if the document may otherwise be released. Staff shall not publicly post or display a document containing a full SSN, except as allowed by state or federal law.

d. Disposing of Personal Information
Staff must properly dispose of or erase Personal Information pursuant to County Administrative Procedure No. 506-A.

e. Reporting
Staff must immediately report any suspected Breach of Security to the Data Security Officer assigned to the Department or the contract administrator for any contractor. In addition, staff must immediately fill out an incident report for any suspected Breach of Security.

2. Data Security Officer Designation:

Department directors must designate at least one Data Security Officer. The Data Security Officer is responsible for the security of Personal Information, reviewing any suspected Breach of Security, reducing its risk of exposure and ensuring that the department's activities do not introduce risk to the County.

3. Violations:

The requirements of the Oregon Consumer Information Protection Act (ORS 646A.600 through 646A.628) are enforced by the State of Oregon, Department of Consumer and Business Services. Violations may result in penalties up to a maximum of $500,000 per occurrence. Violation of this policy and/or County Administrative Procedure No. 506-A by an employee, volunteer, or intern may also constitute just cause for disciplinary action up to and including discharge. Violation of this policy and/or County Administrative Procedure No. 506-A by a contractor is considered a substantive breach of contract and grounds for termination of the underlying contract for cause.

4. Exceptions:

Exceptions may only be granted by the Washington County Board of Commissioners unless such authority has been delegated to the County Administrator.

5. Implementation:

   Elected officials and department directors are expected to be knowledgeable of, and shall be responsible for, implementing this policy within their respective departments. Compliance with this policy is mandatory for all Staff.

6. Periodic Review:

   This policy shall be reviewed by Support Services, Information Technology Division, at least every three years, or more often if needed, and updated as necessary.