

	PROGRAM PROCEDURE P-PPA: PROTECTION OF PERSONAL INFORMATION AND DATA
	DATE: 7/1/2016
	<input checked="" type="checkbox"/> NEW <input type="checkbox"/> REVISED

BACKGROUND

The Office of Management and Budget defines Protected Personally Identifiable Information (PPI) as information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal identifying information that is linked or linkable to a specific individual. Examples of protected PPI include but are not limited to social security numbers (SSN), credit card numbers, bank account numbers, ages, birthdates, medical history, financial history and computer passwords.

As an important and inherent part of the services provided to customers, service providers and WorkSource staff must necessarily collect a wide variety of PPI from customers. While the information collected as a matter of routine is often critical to effectively serving customers and providing them with the best possible services, collection of PPI also brings with it a statutory responsibility to safeguard customers’ PPI from unauthorized use or disclosure.

PROCEDURES

Although an employee may be authorized to access confidential data, the employee may access the data only in connection with the performance of his/her official duties.

Confidential PPI records include entire record systems, specific records or individually identifiable data that are not subject to public disclosure under Oregon Revised Statutes 192, and may include all documents, participant file content, computer files, letters, and other notations of records or data.

Documents that contain PPI (participants’ or family members’) social security numbers, driver’s license, birth certificates, I-9 documents, TANF/FSUP, etc., must be stored in a confidential, locked file cabinet which is only accessible by appropriate staff, kept separate from the working files. The working file may not contain any PPI documents.

Computers that have access to customer data must be locked when not in use and anytime a staff person is away from their workstation.

In Oregon, electronic participant information is stored in the WorkSource Oregon Management Information System (WOMIS) on servers maintained by Oregon Employment Department and

administered under the rules of the Oregon Department of Administrative Services (DAS). Information is also stored in I-Trac which is administered by Worksystems, Inc. Access to these systems and their data is restricted to individuals who have successfully completed DAS Information Security Testing and I-Trac User and Confidentiality Training. All staff with access to either system must follow the procedures set out by the administering agency. Electronic information and data is subject to all the requirements of this policy.