POLICY #: P-02
Protection of Confidential Information and Data

ISSUED: May 17, 2018

PURPOSE
To establish guidelines related to the protection of confidential WIOA Adult, Dislocated Worker, and Youth job seeker information.

REFERENCES
- 2 CFR 200.79 Personally Identifiable Information
- TEGL 39-11 Handling and Protection of Personally Identifiable Information (PII)
- Oregon Revised Statutes 162.425 Misuse of Confidential Information
- Oregon Revised Statutes 192.001 Protection and Storage of Public Records
- Oregon Revised Statutes 660.339 Participant records
- Oregon Revised Statutes 657.665 Confidentiality of Information
- Oregon Revised Statutes 676.177 Interagency shared Information System
- Oregon Administrative Rule 471-010-0105 Customer Information and Disclosure
- Oregon Administrative Rule 589-020.0320 Authority to Request Social Security Numbers
- Oregon Administrative Rule 589-020-0330 Confidentiality

DEFINITIONS
Protected Personally Identifiable Information (PII): The Office of Management and Budget (OMB) defines PII 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 PII include but are not limited to social security numbers, driver’s licenses, birth certificates, I-9 documents, TANF/FSUP records, credit card numbers, bank account numbers, birthdates, medical history, financial history and computer passwords.

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

Maintaining confidential records is important for obvious reasons to the individual, including the prevention of identity theft. Policies and procedures regarding confidentiality and data access must ensure that all necessary and legally permissible data are available to staff who are legally...
authorized to make use of the data in the discharge of their official duties. Protecting the confidentiality of customer information accessed by staff in carrying out official functions of the workforce system is imperative.

All data included in Oregon workforce and employment management information systems (MIS) databases as well as other information data sources available through other partners such as the Department of Human Services (DHS), the Oregon Employment Department UI, etc. is subject to the requirements of these confidentiality statutes. Particular care must be taken to assure that the information and data accessible through the MIS system as well as other data and information sources accessible by service providers and staff is protected and used appropriately.

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.

As used in this policy the term confidential refers to entire record systems, specific records, or individually identifiable data that are not subject to public disclosure under Oregon Revised Statutes 192, Records, Public Records and Meetings. When applicable, confidentiality covers all documents, papers, hard copy participant files, computer files, letters, and all other notations of records or data that are designated by law as confidential.

Documents that contain protected PII must be stored in a confidential, locked file cabinet which is only accessible by appropriate staff. Computers that have access to customer data should be locked when not in use and anytime a staff person is away from their workstation.

Given the integration and merging of services within the WorkSource Centers, confidential information that is received by one WorkSource Oregon partner from another partner agency retains its confidentiality unless otherwise provided by law. The requirement of the program that provides the information shall apply.

In Oregon, the initial participant’s electronic information data is stored in WOMIS on servers maintained by Oregon Employment Department (OED) and administered under the rules of the Oregon Department of Administrative Services (DAS). WIOA participant’s electronic information is kept secure on the I-Trac data servers and administered by Worksystems Inc. Currently subrecipients and OED staff can only access the data on the servers after successful completion of DAS Information Security Testing and I-Trac User and Confidentiality Training. No one should be given access to either WOMIS or I-Trac that have not completed the appropriate training and have signed the appropriate confidentially disclosure. All staff with access to either system must follow the procedures set out by the administering agency, ensuring that all staff understanding of data confidentiality.
Approved:

[Signature]

5.17.18

Clackamas Workforce Partnership Board Chair

Date