Ohio Valley Employment Resource
PO Box 181 Marietta, OH 45750
www.omj15.com
Serving Monroe, Morgan, Noble & Washington Counties Since 2000

Ohio Valley Employment Resource Policy Letter No. 3-15

Use of Personally Identifiable Information

Purpose

This policy is for use by any employee, subcontractor or one-stop partner of Ohio Valley Employment Resource (OVER) who has access to customer information to ensure the security and appropriate use of Personally Identifiable Information (PII). These standards are furnished to ensure that such information is obtained in an effective manner and in compliance with the provisions of applicable federal and state grant/contract requirements, statutes, and executive orders.

I. Effective Date with WDB and COG motion #s

January 1, 2016; COG motion 9-15 on 1/25/16; WDB motion 10-15 on 12/14/15

II. Requirements

Any employee, subcontractor or one-stop partner of Ohio Valley Employment Resource who has access to customer information shall receive, use, secure, maintain, and appropriately destroy Personally Identifiable Information (PII) in strict compliance with all applicable grant requirements, 2 CFR 200, and governmental statutes. Failure to safeguard PII will be reported to the Executive Director of OVER for appropriate reporting and corrective action.

III. Definitions

1) **Personally Identifiable Information** (PII) is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual (OMB Memorandum M-07-16).

i. **Protected PII** – Information that if disclosed could result in harm to the individual whose name or identity is linked to that information. Examples of protected PII include, but are not limited to, SSNs, credit card numbers, bank account numbers, home telephone numbers, ages, birthdates, marital status, spouse names, educational history, biometric identifiers (fingerprints, voiceprints, iris scans, etc.), medical history, financial information and computer passwords.

ii. **Non-sensitive PII** – is information that if disclosed, by itself, could not reasonably be expected to result in personal harm. Essentially, it is stand-alone information that is not linked or closely associated with any protected or unprotected PII. Examples include first and last names, e-mail addresses, business addresses, business telephone numbers, general education credentials, gender, or race. However, depending on the circumstances, a combination of these items could potentially be categorized as protected or sensitive PII.

2) **Sensitive Information** is any unclassified information whose loss, misuse, or unauthorized access to or modification of could adversely affect the interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act.

IV. Requirements

1) Training:

a. Anyone that has, or will have, access to any sensitive/confidential/proprietary/private data must be advised of the confidential nature of the information, the safeguards required to protect the information, and that there are civil and criminal sanctions for noncompliance with such safeguards that are contained in federal and state laws.

b. Employees must acknowledge understanding of this policy and procedure and all required compliance responsibilities before having access to PII.

2) Acquisition of PII:

a. PII must only be received or extracted from data for purposes stated in the grant agreement/contract.

3) Access to and Use of PII:

a. Do not request, secure, or later access or use PII for any purpose other than performing the essential aspects of your job.

b. Do not request any PII that is not required to perform human resources or grant procedures.

c. Transmission or storage of PII via e-mail, flash drives, CDs, DVDs, etc. must be encrypted using Federal Information Processing Standards (FIPS) 140-2 compliant and National Institute of Standards and Technology (NIST) validated cryptographic module. Unencrypted sensitive PII must not be e-mailed to any entity or individual.

d. When obtaining, using, securing, and maintaining PII obtained through grant administration, comply with grant requirements (at a minimum) with additional compliance procedures when required by OVER's policy and procedure.

e. All PII data must be processed in a manner that will protect the confidentiality of the records/documents and is designed to prevent unauthorized persons from retrieving such records by computer, remote terminal, or any other means. Data may be downloaded to, or maintained on, mobile or portable devices only if the data are

encrypted using NIST validated software products based on FIPS 140-2 encryption.

4) Record Retention and Destruction:

a. PII records will be maintained for the period of time as required by applicable grant or contract requirements, governmental regulations including taxing and reporting authorities, and internal human resources requirements, whichever is longer.

b. Record Destruction will be conducted upon completion of the longest record retention requirement applicable to the record.

c. PII records must be stored in an area that is physically safe from unauthorized persons at all times and the data will be processed using grantee-issued equipment, managed information technology (IT) services, and designated locations in compliance with Grantor requirements.

i. Accessing, processing, and storing of PII on personally owned equipment, at off-site locations and non-grantee managed IT services, is STRICTLY prohibited unless approved by grantor.

d. PII will be secured in the WIOA office, in a physically safe location designed to prevent unauthorized persons from accessing or retrieving via any means (including but not limited to computer, mobile device, remote terminal) and its access will be restricted to only those employees charged with protecting or using PII to perform the essential functions of their jobs or per the grant/contract requirements as applicable.

5) On-Site Inspection:

a. OVER and all subcontractors will permit on-site inspections during regular business hours for the purpose of conducting audits and/or to conduct other investigations to assure that the grantee is complying with the confidentiality requirements described in the grant agreement. OVER and all subcontractors will make records applicable to the grant agreement available to authorized persons for the purpose of inspection, review, and/or audit.

6) Failure to Comply:

a. Failure to comply with the requirements or any improper use or disclosure of PII for an unauthorized purpose, may result in the termination or suspension of the grant/contract, or the imposition of special conditions or restrictions, or such other actions as may be deemed necessary to protect the privacy of customers or the integrity of data.

V. References

Specific Grant / Contract Requirements
TEGL 39-11
2 CFR200
Federal / State statutes and regulations.

EMPLOYEE ATTESTATI ON
Personally Identifiable Information (Pll)

I require access to various PII of OVER customers as a function of my employment. I assert that I have read and understand the OVER Pll Policy. I understand my responsibility regarding the proper receipt, access, use, and record retention and destruction of Pll data and records. I will comply with the OVER Pll Policy and immediately report any breeches to OVER's Executive Director so that appropriate reporting and corrective action can be made.

_____ _____
Signature Date

_____ _____
Name Title