Policy on the Handling and Protection of Personally Identifiable Information (PII)

Issue Date: October 21, 2013
Revision Date: July 2016

Purpose:

To provide guidance to 1) the North Central Workforce Development Board staff, 2) One-Stop Operators, 3) subcontracted Workforce Innovation and Opportunity Act (WIOA) programs (hereafter collectively referred to as *local WIOA administrative and service providers*) and, 4) PA CareerLink® Partners staff in compliance with the requirements of handling and protecting PII for customers of the PA CareerLink® centers located in the North Central Workforce Development Area (NC 125) who receive services funded with Federal Department of Labor (DOL) Employment and Training (ETA) funds channeled to the local area directly or through the Commonwealth.

Background: As part of WIOA or other funded grant activities, staff may have in their possession large quantities of Personally Identifiable Information (PII) relating to their organization and staff; and individual program participants. This information is generally found in personnel files, participant data sets, performance reports, program evaluations, grant and contract files and other sources.

As a recipient of WIOA and other Federal and State funds, the North Central Workforce Development Board is required to take aggressive measures to mitigate the risks associated with the collection, storage, and dissemination of sensitive data including PII.

In accordance with federal and state law, individuals applying for WIOA or other funded services must be provided an opportunity to submit authorization which allows the service provider to share their personal and confidential information and records. Each individual must also be informed that they can request their personal and confidential information not be shared among the partner agencies of the PA CareerLink® system and this request does not affect their eligibility for services.

Definitions:

- *PII* – as defined in the Employment and Training Administration's (ETA) Training and Employment Guidance Letter No. 39-11 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.
- *Sensitive Information* – Any unclassified information whose loss, use, misuse, or unauthorized access to or modification could adversely affect the interest or the conduct of Federal programs, or privacy to which individuals are entitled under the Privacy Act of 1974.

- *Protected PII and non-sensitive PII* – DOL has defined two types of PII, *protected PII* and *non-sensitive PII* are primarily based on an analysis regarding the "risk of harm" that could result from the release of the PII.

    1. *Protected PII* is 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, social security numbers (SSNs), credit card numbers, bank account numbers, home telephone numbers, ages, birthdates, marital status, spouse names, educational history, biometric identifiers (fingerprints, voice prints, iris scans, etc.), medical history, financial information, and computer passwords.
    2. *Non-sensitive PII*, on the other hand, 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 of non-sensitive PII include information such as first and last names, email 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.

        To illustrate the connection between non-sensitive PII and protected PII, the disclosure of a name, business email address, or business address most likely will not result in a high degree of harm to an individual. However, a name linked to a social security number, a date of birth, and mother's maiden name could result in identity theft.

<u>Requirements</u>:

Federal law, Office of Management and Budget (OMB) Guidance, DOL and ETA policies require that PII and other sensitive information be protected. To ensure compliance with Federal law and regulations, *local WIA Administrative and service providers* must secure transmission of PII and sensitive data developed, obtained, or otherwise associated with grants/contracts funded by ETA directly or through the state.

In addition to the above requirement, local WIOA administrative and service providers must comply with all of the following:

- To ensure that such PII is not transmitted to unauthorized users, all PII and other sensitive data transmitted via email or stored on CDs, DVDs, thumb drives, etc. must be encrypted using a Federal Information Processing Standards (FIPS) 140-2 compliant and National Institute of Standards and Technology (NIST) validated cryptographic module. Local WIOA administrative and service providers must not email unencrypted sensitive PII to <u>any</u> entity;
- Local WIOA administrative and service providers must take the steps necessary to ensure the privacy of all PII obtained from participants and/or other individuals and to protect such information from unauthorized disclosure. They must maintain such PII in accordance with the standards for information security described in this Policy and any updates to such standards issued by DOL;
- Local WIOA administrative and service providers shall ensure that any PII used during the performance of their grant/contract has been obtained in conformity with applicable Federal and State laws governing the confidentiality of information. They shall further acknowledge that all PII data obtained through grants/ contracts funded with federal monies shall be stored in an area that is physically safe from access by unauthorized persons at all times and the data will be processed using equipment, managed information technology (IT) services, at designated locations approved by the WDB. Accessing, processing, and storing of PII data on personally owned equipment, at offsite locations, e.g. employee's home, and non-grantee managed IT services, e.g. Yahoo mail, is strictly prohibited unless approved by the WIB;

- Employees and other personnel who will have access to 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;
- Local WIOA administrative and service providers must have their policies and procedures in place under which their employees and other personnel, before being granted access to PII, acknowledge their understanding of the confidential nature of the data and the safeguards with which they must comply in their handling of such data as well as the fact that they may be liable to civil and criminal sanctions for improper disclosure;
- Local WIOA administrative and service providers must not extract information from data supplied by their funding source for any purpose not stated in the grant or contract agreement;
- Access to any PII created by the grant or contract funded with Federal monies must be restricted to only those employees of the grant/contract recipient who needs it in their official capacity to perform duties in connection with the scope of work in the grant/contract agreement;
- 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 of the data is encrypted using NIST validated software products based on FIPS 140-2 encryption. In addition, wage data may only be accessed from secure locations;
- PII data obtained by local WIOA administrative or service providers through a request from their funder must not be disclosed to anyone but the individual requestor except as permitted by the grant/contract provider;
- Local WIOA administrative and service providers must permit their funder to make onsite inspections during regular business hours for the purpose of conducting audits and/or conducting other investigations to assure that they are complying with the confidentiality requirements described above. In accordance with this responsibility, local WIOA administrative and service providers must make records applicable to the grant/ contract Agreement available to authorized persons for the purpose of inspection, review, and/or audit; and,
- Local WIOA administrative and service providers must retain data received from ETA-funded grants only for the period of time required to use it for assessment and other purposes, or to satisfy applicable local/state/Federal records retention requirements, if any. Thereafter, the grantee agrees that all data will be destroyed, including the degaussing of magnetic tape files and deletion of electronic data.

An ETA-funded grantee's/subcontractor's failure to comply with the requirements identified in this Policy, 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 the applicable grant/contract administrator may deem necessary to protect the privacy of participants or the integrity of data.

Policy:

Protected PII is the most sensitive information that staff may encounter in the course of their ETA-funded grant/contract work, and it is important that it stays protected. Grantees/subcontractors are required to protect PII when transmitting information, but are also required to protect PII and sensitive information when collecting, storing and/or disposing of information as well. Outlined below are some recommendations to help protect PII:

- Ensure that all staff of all service providers located in the PA CareerLink® centers has reviewed both TEGL 39-11 as well as this policy.
- Ensure that all Staff (present and new) sign and return the Confidentiality agreement and submit to Pam Streich, Director of Planning for the North Central Workforce Development Board.

- Before collecting PII or sensitive information from participants, have participants sign releases acknowledging the use of PII for grant purposes only;
- Whenever possible, ETA recommends the use of unique identifiers for participant tracking instead of SSNs. While SSNs may initially be required for performance tracking purposes, a unique identifier could be linked to each individual record. Once the SSN is entered for performance tracking, the unique identifier would be used in place of the SSN for tracking purposes. If SSNs are to be used for tracking purposes, they must be stored or displayed in a way that is not attributable to a particular individual, such as using a truncated SSN;
- Use appropriate methods for destroying sensitive PII in paper files (i.e. shredding or using a burn bag) and securely deleting sensitive electronic PII;
- Do not leave records containing PII open and unattended;
- Store documents containing PII in locked cabinets when not in use; and,
- Immediately report any breach or suspected breach of PII to the funding source administrator responsible for the grant/contract to Workforce Solutions for North Central PA / North Central Workforce Development Board. See contact information below.

1. **Expiration**
   Ongoing

2. **Inquiries**
   Questions shall be directed to: Susan R. Snelick ssnelick@ncwdb.org (814)245-1835 ext. 101
   or Pamela A. Streich pstreich@ncwdb.org (814)-245-1835 ext. 102

Auxiliary aids and services available upon request to individuals with disabilities.
Equal Opportunity Employer / Program