Administrative Policy #1002
Protection of Personally Identifiable Information (PII)

Date Issued: 10/18/2013 **Date Effective:** 10/18/2013 **Date of Last Revision:** 01/12/2018

I. Purpose

This policy will provide detailed guidance for the use and protection of all Personal Identifiable Information (PII) provided as part of the intake and delivery of PA CareerLink® and/or Workforce Innovation and Opportunity Act (WIOA) services to individuals.

II. Background

The Local Workforce Development Area (LWDA)/ Local Workforce Development Board (LWDB) is required by USDOL Employment and Training Administration's (ETA) Training and Employment Guidance Letter (TEGL) No. 39-11, *Guidance on the Handling and Protection of Personally Identifiable Information (PII)* and BWDP Director Email dated 06/17/2013 (Appendix A) to protect PII when transmitting information, and protect PII sensitive information when collecting, storing and/or disposing of information.

III. Definitions

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 or identifying information that is linked or linkable to a specific individual.

Sensitive Information – 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.

Protected PII and non-sensitive PII - DOL has defined two types of PII, protected PII and non-sensitive PII. The differences between 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, voiceprints, 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; 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. For example, the disclosure of a name, business e-mail address, or business address most likely will not result in a high degree of harm to an individual. *However, depending on*

the circumstances, a combination of these items could potentially be categorized as "protected or sensitive PII".

A name linked to a social security number, a date of birth, and mother's maiden name could result in identity theft. This demonstrates why protecting the information of PA CareerLink® and WIOA program participants is so important.

IV. Roles and Responsibilities

All staff (hereinafter refers to WCJP **and** Contractor staff) having access to Personal Identifiable Information (PII) of PA CareerLink® and/or WIOA applicants/participants must abide by this protection policy, TEGL 39-11 and the email from the BWDP Director referenced in the Background section of this policy.

Staff is **required** to protect sensitive PII when transmitting information **AND** when collecting, storing and/or disposing of information. Access to any PII must be restricted to only those employees (WCJP and Contractor) who need the information in their official capacity to perform duties in connection to PA CareerLink® and/or WIOA activities. To ensure that sensitive PII is not transmitted to unauthorized users, all PII and other sensitive data transmitted via email must be encrypted. No sensitive PII and other sensitive data may be stored on CDs, DVDs, thumb drives, etc. Sensitive PII **cannot** be sent in clear text even in Excel spreadsheet attachments.

All PII data **must** be processed in a manner that will protect the confidentiality of the records/documents to prevent unauthorized persons from retrieving such records by computer, remote terminal or any other means. Personal Identification (PID) numbers assigned by the Comprehensive Workforce Development System (CWDS) should always be used INSTEAD of the individual's Social Security Number (SSN) when identifying an applicant/participant. All staff (WCJP and Contractor) **must** utilize the SendInc plug-in to encrypt and send sensitive PII via Outlook email to any other WCJP staff, contracted staff or other agencies. WCJP staff is limited to 20 encrypted emails per day.

Records, documents and paperwork containing PII should not be left on computers or in the open unattended where unauthorized persons (other applicants/participants, coworkers, cleaning personnel, etc.) would have the capability of reading, copying, etc. Records, documents and paperwork containing PII ***MUST BE SECURED*** in locked file cabinets, desks or offices when unattended.

PII should not be taken to an employee's home or off-site location with the exception of contracted sites. Staff and contracted sites 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 non-compliance with such safeguards contained in Federal and State laws. Accessing, processing and storing PII data is prohibited on: flash drives; personally owned equipment; off-site locations such as the employees' (WCJP and Contractor) homes; and on non-employer managed IT services, such as Yahoo or Google Mail accounts.

All PII records and supporting documents must be shredded after the time period required for the records and supporting documents to be retained.

As required by CWDS FR 11.3, WIOA Title I application eligibility documentation is to be uploaded onto CWDS. Documentation will be scanned into a multi-function printing (MFP) device and sent to the appropriate e-mail account. All WCJP MFP devices are outfitted with HDD Data Erase Scheduler V3.1.1. This product provides PII security by erasing the hard drives of MFP devices at scheduled intervals. Staff receiving PII from MFP's are required to only store PII on authorized computers with adequate security in place. Once the information is uploaded onto CWDS and applications are approved, staff are required to delete the information completely from their computers. This will be periodically monitored for compliance.

V. Appendix

Appendix A – Letter from BWDP Director Email dated 06/17/2013

***Sent on behalf of Dmitry Zhmurkin:* June 17, 2013**

To: LWIA WIB Directors; LWIA Participant Reporting Contacts; PCS POCs List; Title I Contractors; Youth Coordinators; CCS POCs; LWIA Fiscal Agents

Please share this information with <u>all</u> Staff and Partners.

Recently, it was brought to the attention of BWDP that *unprotected, confidential* **Personally Identifiable Information (PII)** was being communicated to external partners via unsecured email. In addition, paperwork from multiple participants, containing confidential information, was accessible to other customers, and/or the cleaning crew on employee desk areas. One customer even refused to put their Social Security Number (SSN) on *any* form because of seeing *other* individual's **PII** on an employee's desk. **This is a violation of both Commonwealth and L&I Information Security policy.**

PII is defined as 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. Such as Sensitive Information, 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.

The Department of Labor has defined two types of **PII: Protected PII** and **Non-sensitive PII.** The differences between **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**.

- **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, voiceprints, iris scans, etc.), medical history, financial information and computer passwords.
- **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, e-mail addresses, business addresses, business telephone numbers, general education credentials, gender, or race. <u>*However, depending on the circumstances, a combination of these items could potentially be categorized as "protected or sensitive PII".*</u>

To illustrate the connection between **Non-sensitive PII** and **Protected PII**, the disclosure of a name, business e-mail 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 (SSN), a date of birth, and mother's maiden name could result in *identity theft*. **This demonstrates why protecting the information of our program participants is so important.**

LWIAs/LWIBs are **<u>required</u>** to protect **PII** when transmitting information and are also required to protect **PII** sensitive information when collecting, storing and/or disposing of information as well. 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. If for example, a Social Security Number (SSN) is required to be communicated via

e-mail, LWIAs/LWIBs are **required** to utilize email encryption. In addition, **do not** leave records containing **PII** opened and unattended. Paperwork with confidential information must be secured in locked file cabinets. Use the Participant Identification (PID) number whenever possible, not the SSN. Also, confidential data **cannot** be sent in clear text even in Excel spreadsheet attachments.

Please review **TEGL 39-11,** dated **June 28, 2012** for additional information. To view and/or print **Guidance on the Handling and Protection of Personally Identifiable Information (PII)** please click on the following website address: http://wdr.doleta.gov/directives/attach/TEGL/TEGL_39_11.pdf

Failure to comply with the requirements identified in this **TEGL**, or any improper use or disclosure of **PII** for an unauthorized purpose, may result in the termination or suspension of funds, or the imposition of special conditions or restrictions, or such other actions as the Grant Officer may deem necessary to protect the privacy of participants or the integrity of data.

If you have any questions or require additional clarification, please contact WIA Services at RA-LI-BWDP-PCS@pa.gov

Dr. Dmitry Zhmurkin | Director
Bureau of Workforce Development
Pennsylvania Department of Labor & Industry
651 Boas Street | Harrisburg, PA 17121
Phone: 717.787.3354 | Fax: 717.783.7115
www.dli.state.pa.us