New Jersey
Workforce Innovation Notice 6-15

TO: Workforce Development Board Directors
One-Stop Operators
Employment Service Managers

FROM: John Bicica, Chief,
Office of WIOA Technical Assistance and Capacity Building

DATE: November 2, 2015

References: 20 CFR 683.220; Training and Employment Guidance Letter 39-11

Purpose

To inform all local workforce development areas and one-stop partners of the requirements regarding the handling and protections of personally identifiable information (PII). Compliance with these requirements will be monitored by the New Jersey Department of Labor and Workforce Development. Any noncompliance with the requirements provided in this guidance is subject to corrective action.

Background

The United States Department of Labor Employment and Training Administration has provided requirements regarding the handling of personally identifiable information through the issuance of Training and Employment Guidance Letter (TEGL) 39-11 and in the proposed WIOA rules at 20 CFR 683.220. This guidance provides the requirements in 20 CFR 683.220 and key provisions of TEGL 39-11.

Definitions- TEGL 39-11 provides the following definitions**:**

PII- 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 interests or the conduct of Federal programs, or the privacy to which individuals are entitled to under the Privacy Act.

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, **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-Information that, if dislocated by itself, could not reasonable 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.

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, a date of birth, and mother's maiden name could result in identity theft.

WIOA Requirements

20 CFR 683.220 provide the following requirements:

(a) Recipients and subrecipients of WIOA Title I and Wagner-Peyser Act funds must have an internal control structure and written policies in place that provide safeguards to protect personally identifiable information, records, contracts, grant funds, equipment, sensitive information, tangible items, and other information that is readily or easily exchanged in the open market, or that the Department or recipient or subrecipient considers to be sensitive, consistent with applicable Federal, State and local privacy and confidentiality laws. Internal controls must also include reasonable assurances that the entity is:

(1) Managing the award in compliance with Federal statutes, regulations, and the terms and conditions of the Federal award;

(2) Complying with Federal statutes, regulations, and the terms and conditions of the Federal; awards;

(3) Evaluating and monitoring the recipients' and sunbrecipients; compliance with the statute, regulations and terms and conditions of the federal awards, and;

(4) Taking prompt action when instances of noncompliance are identified.

(b) Internal controls should be in compliance with the guidance in Standards for Internal Control in the Federal Government" issued by the Comptroller General of the United States and the "Internal Control Integrated Framework" issued by the Committee of Sponsoring Organizations of the Treadway Commissions (COSO)

TEGL 39-11 provides the following guidance regarding sensitive PII:

- To ensure compliance that (sensitive) PII is not transmitted to unauthorized users, all PII and other sensitive data transmitted via e-mail or stored on CDs, DVDs, thumb drives, etc., must be encrypted using Federal Information Processing Standards (FIPS) 140-2 compliant and National Institute of Standards and Technology (NSIT) validated cryptographic module. Grantees must not e-mail unencrypted sensitive PII to any entity, including ETA or contractors.

Reminder-Most word processing and spreadsheet applications allow for the encryption of a document, requiring a password for access. When transmitting encrypted information, the password used to access the information must be transmitted in a separate communication.

- Grantees 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. Grantees must maintain such PII in accordance with the ETA standards for information security described in (TEGL 39-11) and any updates to such standards provided to the grantees by ETA.

- Grantees shall ensure that any PII used during the performance of their grant has been obtained in conformity with applicable Federal and State laws governing the confidentiality of information.

- Grantees further acknowledge that all PII data obtained through their ETA grant 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 grantee issued equipment, managed information technology (IT) services, and designated locations approved by ETA. Accessing, processing and storing of ETA Grant PII data on personally owned equipment, at off-site locations e.g employee's home, and non-grantee managed IT services, e.g. Yahoo mail, is strictly prohibited unless approved by ETA.

- Grantee 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.

- Grantees must have their policies and procedures in place under which grantee employees and other personnel, before being granted access to PII, acknowledge their understanding of their 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 for civil and criminal sanctions for improper disclosure.

Recommendations-TEGL 39-11 provides the following recommendations**:**

- 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. Note: the America's One-Stop Operating System (AOSOS) Identification Number is a unique identifier, and can be used in place of SSNs where appropriate. While SSNs may initially be required for performance tracking purposes, a unique identifier could be linked to the 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 pater 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.

Additional PII requirements are addressed in detail in TEGL 39-11 which can be accessed through the following link: http://wdr.doleta.gov/directives/attach/TEGL/TEGL_39_11_Acc.pdf The attachment to the TEGL, an appendix of Federal laws and policies related to data security, can be accessed here http://wdr.doleta.gov/directives/attach/TEGL/TEGL_39_11_Att.pdf

Other Requirements

- Locally developed WIOA forms must not require the recording of Social Security numbers.
- All *original* documents used for eligibility documentation must be returned to the customer.

Action Required

Local workforce development areas must ensure that they develop the internal control structure and written policies required by 20 CFR 683.220. They must additionally ensure that these policies are shared with all partners and contractors, and are incorporated into all memoranda of understanding, contracts and other agreements. LWD, Workforce Development, Field Services, will develop the written polices for Wagner-Peyser programs to ensure compliance with these requirements.

Written policies and procedures for handling of PII. These procedures must include, and each local are must be able to demonstrate compliance with the following:

1. Written policies and procedures are developed and incorporated into all agreements.
2. All PII is stored in an area safe from access by unauthorized individuals
3. PII is not processed on unauthorized equipment
4. There is no transmission of unencrypted PII
5. Forms, folders and other paper documents do not include SSNs

Additional Resources

Standards for Internal Control in the Federal Government –This document may be accessed through the following link: http://www.gao.gov/assets/670/665712.pdf

Internal Control Integrated Framework-Executive Summary-This document may be accessed though the following link: http://www.coso.org/documents/990025P_Executive_Summary_final_may20_e.pdf \

C**OSO Internal Control Framework Poster-**
http://www.coso.org/documents/COSO%20ICIF%2011x17%20cube%20graphic.pdf

Authority

New Jersey Department of Labor and Workforce Development	**X**
State Employment And Training Commission	

Questions

For questions regarding this guidance, contact John Bicica, Chief, Office of WIOA Technical Assistance and Capacity Building, at john.bicica@dol.nj.gov