BURLINGTON COUNTY WORKFORCE DEVELOPMENT BOARD

PERSONALLY IDENTIFIABLE INFORMATION (PII) POLICY

DATE: August 9, 2022

PURPOSE

The Burlington County Workforce Development Board, as the Governor's chosen administrative entity for the Workforce Innovation and Opportunity Act in Burlington County, provides this issuance as guidance regarding Personally Identifiable Information (PII).

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, NJ WIN 6-15, and 20 CFR 683.220.

DEFINTIONS

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 the 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 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.

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. This demonstrates why protecting the information of our program participants is so important.

REQUIREMENTS

Federal Law, OMB Guidance, and Departmental and ETA policies require that PII and other sensitive information be protected. 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. The local area has in place internal controls that 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 subrecipients compliance with the statute, regulations and terms and conditions of the federal awards.

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

(b) Internal controls follow 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)

In addition to the requirements above, the local area will also comply with all of 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.
- The local area will 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.

- The local area will 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. The local area 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.

- The local area will 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.

- The local area further acknowledges 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.

- Local Area employees and other personnel who will have access to sensitive/confidential/proprietary/private data have been 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.

- The local area has policies and procedures in place under which the local area 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.

- 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.

- The local area retains data received from ETA only for the period of time required to use it for assessment and other purposes, or to satisfy applicable Federal records retention requirements, if any. Thereafter, the local area agrees that all data will be destroyed, including the deletion of electronic data.

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, or the imposition of special conditions or restrictions.

Recommendations: Protected PII is the most sensitive information that you may encounter in the course of your grant work, and it is important that it stays protected. The local area and staff 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 the steps that the local area is taking to help protect PII:

- Before collecting PII or sensitive information from participants, participants sign releases acknowledging the use of PII for grant purposes only.
- Whenever possible, the local area will use unique identifiers for participant tracking instead of SSNs. Note: the America's One-Stop Operating System (AOSOS) Identification Number is a unique identifier and will be used in place of SSNs where appropriate. While SSNs may initially be required for performance tracking purposes, a unique identifier (AOSOS number) will 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.
- The local area will not use or develop forms that require the use of Social Security numbers.
- All original documents used for eligibility documentation will be returned to the customer
- Use appropriate methods for destroying sensitive PII in paper files (i.e. shredding) 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.

NOTE

This policy is shared with all partners and contractors, and are incorporated into all memoranda of understanding, contracts, and other agreements.

REFERENCES

- 20 CFR 683.220
- TEGL 39-11
- NJWIN 6-15