Cumberland County Department of Workforce Development

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

Definition of Personally Identifiable Information (PII) – TEGL 39-11 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 - 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.

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.

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:

- To ensure that such 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. Cumberland County Department of Workforce Development (CC DWD) employees must not e-mail unencrypted sensitive PII to any entity, including ETA. Note: 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 only form that will contain a full social security number will be the Customer Registration Form. All other forms will only contain the last four digits of the customer's social security number.
- Do not leave records containing PII open and unattended.
- Store documents containing PII in locked cabinets when not in use.
- CC DWD employees 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.
- CC DWD employees shall ensure that any PII has been obtained in conformity with applicable Federal and state laws governing the confidentiality of information.
- CC DWD employees further acknowledge that all PII data obtained shall be stored in an area that is physically safe from access by unauthorized persons at all times. Accessing, processing, and storing of 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.
- CC DWD 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.
- CC DWD employees must not extract information from data supplied by ETA for any purpose not stated in the grant agreement.
- Access to any PII created by an ETA grant must be restricted to only those employees who need it in their official capacity to perform duties in connection with the scope of work in the grant agreement.
- CC DWD must retain 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 grantee agrees that all data will be destroyed, including the deletion of electronic data.
- Whenever possible the use of unique identifiers for participant tracking instead of SSNs. While SSNs may initially be required for performance tracking purposes, a unique identifier should 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.
- Immediately report any breach or suspected breach of PII to your supervisor.