NWPA JOBCONNECT DISCOVER OPPORTUNITY

NWPA WDB POLICY - 306
Rev. Level: D

Personally Identifiable Information (PII) Policy

The local workforce development board's (LWDB) Personally Identifiable Information (PII) Policy will provide guidance for compliance in handling and protecting PII in the local workforce investment area. This policy applies to all LWDB program oversight provider staff, contractor staff, grantees, sub-grantees, and any other individuals or groups involved in the handling and protecting of personally identifiable information per governing guidelines including federal law, OMB guidance, United States Department of Labor, Employment and Training Administration policies (see Training and Employment Guidance Letter No. 39-11), as well as any relevant state and local requirements.

As part of grant activities, LWDB program oversight provider staff, contractor staff, grantees, sub-grantees and other individuals or groups may have in their possession personally identifiable information (PII) relating to their organization and staff, subgrantee and partner organizations 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. Federal law, OMB guidance, federal, state and local policies require that PII and other sensitive information be protected. To ensure compliance with these policies/regulations, PII and sensitive data developed, obtained or otherwise associated with grantee funding must be secured and protected at all times.

1) All parties 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.

2) All parties must ensure that PII used during the performance of their grant has been obtained in conformity with applicable Federal and state laws governing the confidentiality of information.

3) All parties must acknowledge that all PII data obtained through their program activity shall be stored in an area that is physically safe from access by unauthorized persons at all times and be managed with appropriate information technology (IT) services and designated locations. 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 such as Yahoo mail) is strictly prohibited.

4) All parties 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 within the Federal and state laws.

5) All parties who have access to PII are required to sign a disclosure acknowledging the confidential nature of the data and must comply with safe and secure management of the data. These disclosures must be kept on file with the program service contractor for monitoring review at the request of the LWDB.

6) All parties must 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.

7) Access to any PII through program and grant activity must be restricted to only those employees of the grant recipient who need it in their official capacity to perform duties in connection with the scope of work in the grant agreement.

8) 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.

9) To ensure that 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.

10) All PII data must be retained to satisfy all required record retention requirements. Thereafter, all PII data must be destroyed, including the degaussing of magnetic tape files and deletion of electronic data.

11) With regard to personally identifiable information handled during the provision of Mobile CareerLink services, procedure must be followed as developed and implemented by the one stop operator and approved by the WDB. This procedure will be reviewed annually by the one stop operator and the WDB.

DEFINITIONS

Personal Identifiable Information (PII): 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: 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 educational 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. This demonstrates why protecting the information of our program participants is so important.

RECOMMENDATIONS

- Before collecting PII or sensitive information from participants, have participants sign releases acknowledging the use of PII for grant purposes only.

- Whenever possible, use 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) 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.

- Immediately report any breach or suspected breach of PII.

REFERENCE
USDOL Training and Employment Guidance Letter (TEGL) No. 39-11

HISTORY

Name	Date	Rev. Level	Description of change	Effective Date
Deb O'Neil	11/14/2013	A	New policy based on state requirement	
Deb O'Neil	01/15/2015	B	Revise language, logo	02/25/2015
Deb O'Neil	03/15/2017	C	Revise language per WIOA	06/09/2017
Deb O'Neil	09/20/2017	D	Add language re: mobile services	10/13/2017

Personally Identifiable Information Sign Off Form

I have reviewed and acknowledge the local workforce development board's Personally Identifiable Information Policy and agree that all necessary steps will be taken to ensure the privacy and confidential nature of all personally identifiable information to protect such information from unauthorized disclosure.

I further agree that all personally identifiable information will be stored in an area that is physically safe from access by unauthorized persons at all times, and be managed with appropriate information technology (IT) services and designated locations. Access to any personally identifiable information through program and grant activity will be restricted to only those individuals who need access in their official capacity to perform duties in connection with the scope of work.

_____
Printed Name

_____
Signature

_____
Agency Name

_____
Date

PERSONALLY IDENTIFIABLE INFORMATION PROCEDURES

Any partner staff member providing any PA CareerLink® services outside of a comprehensive site will ensure that they follow NWPA Job Connect Personally Identifiable Information (PII) Policy. All staff members must sign a PII Sign-Off form (included at the end of the aforementioned policy) and a Confidentiality Form. In addition, staff will comply with the following procedures to ensure PII protection while delivering services in the community.

PARTICIPANT FILE PROTECTION

Participant Files will stay in appropriate CareerLink comprehensive sites.

Staff will scan PII documents and store them on the computer versus transporting the documents and will use electronic signature equipment to drastically reduce and eventually eliminate the need for printing and transporting. Any exception to this policy must be reviewed on a case-by-case basis and granted in writing by a manager.

If an exception is granted, participant files (and any other documents containing PII) may only be transported in a visibly locked box, provided by the contractor for mobile operations. No other methods of paper file protection will be recognized as compliant with these procedures. A file check-out form must be completed and left in place of the file in its original location. Additionally, the file transport must be tracked on a document control summary form easily accessed by other staff at the file's original comprehensive site. When the file is returned, the file check-out form may be removed and filed with the document control summary form. The return of the file must be acknowledged on both the check-out form and the document control summary.

CONFIDENTIAL INTERACTION

Staff will be cognizant of the fact that they are having confidential conversations including PII and sensitive information with participants in sometimes public places and will ensure discretion is used at all times. Some methods of employing discretion in a public setting include keeping voices at a low volume or pointing to, writing, or typing sensitive information instead of speaking it aloud.

Sometimes, forms must be printed for participants to fill out. These forms should be scanned after they are completed, and the original given to the participant to ensure it is not accessible by anyone else. These original forms are not to be transported.

EQUIPMENT PROTECTION

Staff will use secure computers, printers and scanners provided by the contractor for mobile operations while working with participants in the community. Please protect this equipment and never leave it unattended and/or available for unauthorized use. Do not share your password. If any equipment is missing, please report the product, equipment ID#, and a description of the situation to your manager immediately, even before taking further steps to retrieve the equipment.