

Policy Name: Personal Identifiable Information (PII) Policy

Policy #: BGWIOA-N16-O9

Effective Date: October 12, 2016

Applies to: Adults, Dislocated Workers, Older Youth, Trade

1. **Purpose:** To provide guidance to WIOA staff on compliance requirements of handling and protecting PII of their participants based on guidance established by the Commonwealth of Kentucky.
2. **Background:** WIOA staff handle large amounts of PII relating to their clients on a daily basis. This information is generally found in participant files, participant data sets, lists, performance reports, program evaluations, etc.
3. **Definitions:**
 - PII – 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.
 - Sensitive Information – any information whose loss, misuse or unauthorized access to or modification of could adversely affect the interest or conduct or the privacy to which individuals are entitled under the Privacy Act.
 - Protected PII and non-sensitive PII – the Department of Labor (the Department) 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, spouses names, educational history, biometric identifiers (fingerprints, voiceprints, 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 standalone information that is not linked closely with any protected or unprotected PII. Examples of non-sensitive PII include information such as first and last names, email 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 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 a mother’s maiden name could result in identity theft. This demonstrates why protecting the information of our program participants is so important.

4. **Policy:** PII and other sensitive information are required to be protected. As stewards of Federal funds, handling of PII and sensitive information and has to be in compliance with the Federal law and regulations, staff must secure transmission of PII and sensitive data developed, obtained, or otherwise associated with the WIOA program.

In addition to the requirements above, all WIOA staff must also comply with all of the following:

- *To ensure that such 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. WIOA staff shall not email unencrypted sensitive PII to any entity, internally or externally.*
- *WIOA staff must take steps necessary to ensure the privacy of all PII obtained from participants and/or other individuals and to protect such information from unauthorized disclosure. WIOA staff must maintain such PII in accordance with the standards described in this policy and any updates to such standards provided to the WIOA staff by future updates.*
- WIOA staff shall ensure that any PII used during the performance of their duties has been obtained in conformity with this policy.
- WIOA staff further acknowledge that all PII data obtained through their duties 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 WIOA authorized equipment, managed WIOA approved information technology (IT) services, and designated locations approved by the WIOA program.
- WIOA staff 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.
- WIOA staff must receive training on this policy and the procedures for dealing with confidential information, before being granted access to PII 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.
- WIOA staff must not extract information from data supplied for any purpose not stated as part of their duties.
- Access to any PII created in the line of their duties must be restricted to only those employees who need it in their official capacity to perform duties in connection with the scope of Workforce and held under the same restrictions for PII through the Department of Labor.
- *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. Data may be downloaded to, or maintained on, mobile portable devices if the data is encrypted. In addition, wage data may only be accessed from secure locations.*
- PII data obtained by WIOA staff through a request must not be disclosed to anyone but the individual requestor and those permitted under this policy.
- WIOA administrative staff will make onsite inspections during regular business hours for the purpose of conducting monitoring to ensure that staff are complying with confidentiality requirements described above. In accordance with this responsibility, WIOA staff must make records applicable to this policy available to authorized persons for the purpose of inspection, review, and/or monitoring.
- WIOA staff must retain data 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, WIOA staff agrees that all data will be destroyed, including the any electronic data.
- Use the participant's KY# for participant tracking instead of SSN. While SSNs may initially be required for performance tracking purposes, a unique identifier (such as KY#) could be linked to each individual record. Once the SSN is entered for performance tracking, the unique identifier should be used in place of the SSN for tracking purposes.
- Use appropriate methods for destroying sensitive PII in paper 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.
- Immediately report any breach or suspected breach of PII to the Director of Workforce Services or Assistant Director of Workforce Services.

WIOA staff's 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 that individual.