Kentucky Career Center

GUIDANCE

COMMONWEALTH OF KENTUCKY
DEPARTMENT OF WORKFORCE DEVELOPMENT

GUIDANCE NAME: Handling and Protection of Personally Identifiable Information (PII)

GUIDANCE NUMBER: 24-002
DATE OF REISSUE: June 1, 2024
EFFECTIVE DATE: June 1, 2024

APPLIES/OF INTEREST TO: Kentucky Career Center (KCC) Staff and Local Workforce Development Area (LWDA) staff

POINT OF CONTACT: Division of Technical Assistance, compliance.unit@ky.gov

HISTORY: As part of their grant activities, WIOA funded agencies (including WIOA service providers) may have in their possession large quantities of PII relating to their organization and staff; partner organizations and their 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. All parties in possession of PII are required to take aggressive measures to mitigate the risks associated with the collection, storage, and dissemination of PII.

PURPOSE: The purpose of this policy is to provide guidance on compliance with the requirements of handling and protecting personally identifiable information (PII).

PROCEDURAL GUIDANCE: Federal regulations require that PII and other sensitive information be protected. All WIOA funded agencies (including WIOA service providers) must secure transmission of PII and sensitive data developed, obtained, or otherwise associated with WIOA funds and must comply with all of the following:

- Ensure PII is not transmitted to unauthorized users and all PII and other sensitive data transmitted via e-mail or stored on CDs, DVDs, thumb drives, etc., must be encrypted.
- Take the necessary steps to ensure the privacy of all PII obtained from participants and/or other individuals and to protect such information from unauthorized disclosure.
- Ensure that any PII is obtained in conformity with applicable Federal and state laws governing the confidentiality of information.

- Acknowledge that all PII data 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 (i.e. employee's home, personal email), is strictly prohibited unless approved by ETA.
- Ensure all employees and other personnel who will have access to sensitive, confidential, proprietary, and/or private data are: (1) advised of the confidential nature of the information and of the safeguards required to protect the information; and (2) are advised that, per Federal and state laws, civil and criminal sanctions may be imposed for noncompliance.
- Have in place policies and procedures under which all employees and other personnel acknowledge (1) their understanding of the confidential nature of the data; (2) the requirements with which they are required to comply when handling such data; and (3) that they may be liable to civil and/or criminal sanctions for noncompliance with statutory nondisclosure requirements.
- Must not extract information from data supplied by the case management system of record for any purpose not stated in the grant or agreement with the Education and Labor Cabinet.
- Access to any PII 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 or agreement. Retain all records pertinent to applicants, registrants, eligible applicants/registrants, participants, terminations, employees, and applicants for employment for not less than three years from the close of the applicant program year (the year in which the applicant applied for the program). Such records must be maintained as a whole record system.
- 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 or portable devices only if the data are encrypted.
- Must permit Federal and or state staff to make onsite inspections during regular business hours for the purpose of conducting audits and/or conducting other investigations to assure that the WIOA funded agency is complying with the confidentiality requirements described in this policy.
- Must retain data received 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 degaussing of magnetic tape files and deletion of electronic data.
- Protected PII is the most sensitive information encountered in the course of grant work, and it is important that it stays protected. WIOA service providers and funded agencies 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 some recommendations to help protect PII:

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

  o 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 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.

  o Use appropriate methods for destroying sensitive PII in paper files (i.e., shredding) and securely deleting sensitive electronic PII.

  o Do not leave records containing PII open and unattended

  o Store documents containing PII in locked cabinets when not in use.

  o Immediately report any breach or suspected breach of PII to the Policy and Audit Branch of the Education and Labor Cabinet.

REQUIRED ACTION: Reference the following page of this policy for guidance on the handling and protection of personally identifiable information (PII)..

REFERENCES:

U. S. Department of Labor (DOL), Employment and Training Administration (ETA), Training and Employment Guidance Letter (TEGL) 39-11, Guidance on the Handling and Protection of Personally Identifiable Information (PII) (June 28, 2012).