1601POL Protection of Personally Identifiable Information (PPII) (Rev1)

Effective Date: November 2020
Last Modified: July 2024

To provide services to job seekers and other WorkSource System customers, Olympic Workforce Development Council (OWDC) staff, subrecipients, contractors and partners collect and store a variety of protected, personal identifiable information (PII). OWDC is committed to ensuring appropriate use, storage, and protection of PII from unauthorized use or disclosure that align with federal Workforce Innovation and Opportunity Act (WIOA) law, regulation, and guidance

1. **Confidential PII Records** include entire record systems, specific records or individual identifiable data.
   a. Records may include; documents, file content, computer files, letters, and other notations of records or data.
2. **Subrecipients are required to employee proactively methods for protecting PII, including internal controls and written policies and procedures for safeguarding PII in compliance with 2 CRF 200.303. Including methods for collecting, maintaining, storing, purging, and securely transmitting PII.**
3. **Protection of PII: Physical documents that contain PII,** such as (participants' or family members') social security numbers, driver's license, birth certificates, or I-9 documents, must be stored in a confidential, locked file cabinet, only accessible by appropriate staff.
   a. At no time should any staff retain PII on personal devices or unsecured networks.
   b. **Computers that have access to PII data** must be locked when not in use and anytime a staff person is not attending their workstation.
   c. **All staff with access to online systems containing PII** must follow the procedures established by the administering agency. Electronic information and data are subject to all the requirements of this policy.
4. **Staff and subrecipients are required to ensure the privacy of all PPII and to protect such information from unauthorized disclosure.** Loss of PII can result in substantial harm to individuals, including identify theft or other fraudulent use of this information.
   - Maintain PII in accordance with the standards for information security described in *TEGL 39-11.*
   - Ensure that during the performance of each grant/contract, PII has been obtained in conformity with applicable Federal and State laws governing the confidentiality of information.
   - If improper use of PII or unauthorized access to PII occur, staff are required to immediately notify OWDC Program Supervisor and Program Analyst of the breach. OWDC staff will take required action to notify partner agencies and corrective action plans will be issued.
5. **Failure to comply with the *TEGL 39-11* requirements may result in disciplinary action.**
   - Subrecipient's improper use of PII for an unauthorized purpose, may result in the termination or suspension of the contract, the imposition of special conditions or restrictions, or other actions the OWDC deem necessary to protect the privacy of participants or the integrity of data.

References

Guidance on the Handling and Protection of Personally Identifiable Information, Training and Employment Guidance Letter, TEGL 39-11

Personally Identifiable Information, Subpart A – Acronyms and Definitions, Code of Federal Regulations Title 2, Subtitle A, Chapter 11 Part 200, 2 CFR §200.79 & 2 CRF § 200.303.

Records Retention and Public Access, Workforce Innovation and Opportunity Act Policy 5403 (Rev1) Safeguarding Personally Identifiable Information (PII), WorkSource System Policy 1026