PARTNER4WORK

PERSONALLY IDENTIFIABLE INFORMATION POLICY (PII)

Purpose

As part of grant activities, staff may have access to program participant or staff PII. This information is generally found in personnel files, participant data sets, performance reports, program evaluations, grant and contract files, or other sources. Federal law and federal policies require that PII and other sensitive information be secured and protected at all times.

Affected Parties

This policy applies to all Partner4Work staff, contractor staff, grantees, sub-grantees, and any other individuals or groups involved in the handling and protecting of Personally Identifiable Information (PII) for programs serving participants who receive Workforce Innovation and Opportunity Act (WIOA), Temporary Assistance for Needy Families (TANF), and other public and private funds.

References

- TEGL 39-11

Definition of Key Terms

OMB defines "Personally Identifiable Information" (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.

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" is information that if disclosed, by itself, could not reasonably be expected to result in personal harm. It is standalone 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.

Eligibility Requirements

PII from all participants and potential participants must be protected at all times. There is no eligibility requirement.

Policy

All parties must ensure the privacy of all PII obtained from participants and to protect such information from unauthorized disclosure. All parties must ensure that PII used during their grant has been obtained in conformity with applicable Federal and state laws and policies governing the confidentiality of information.

All PII transmitted via e-mail or stored on external drives must be encrypted. All PII stored onsite must be kept safe from unauthorized individuals at all times and must be managed with appropriate information technology (IT) services. 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, Gmail, etc.) is strictly prohibited.

All parties who will have access to sensitive/confidential/proprietary/private data must be advised of the confidential nature of the information, the safeguards with which they must comply to protect the information, and that they may be liable to civil and criminal sanctions for improper disclosure.

Access to any PII obtained through the grant 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.

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.

Grantees must permit the Employment and Training Administration (ETA) and Partner4Work to make onsite inspections during regular business hours for the purpose of conducting audits and/or conducting other investigations to assure that the grantee is complying with the confidentiality requirements described above. In accordance with this responsibility, grantees must make records applicable to this agreement available to authorized persons for the purpose of inspection, review and/or audit.

Grantees must retain data received from ETA or Partner4Work only for the period of time required to use it for assessment and other purposes, or to satisfy applicable Federal and Partner4Work records retention requirements, if any. Thereafter, the grantee agrees that all data will be destroyed, including deletion of electronic data.

Additional Requirements:

1. Before collecting PII or sensitive information from participants, have participants sign releases acknowledging the use of PII for grant purposes only.
2. 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.
3. Use appropriate methods for destroying sensitive PII in paper files (i.e. shredding) and securely deleting sensitive electronic PII.
4. Do not leave records containing PII open and unattended.
5. Store documents containing PII in locked cabinets when not in use.
6. Immediately report any breach or suspected breach of PII.

Effective Date: July 1, 2018