Policy Number: P-WIOA-PPSI-1.A
Effective Date: April 11, 2017
Approved By: Nick Schultz, Executive Director

Protecting Personal and Sensitive Information

PURPOSE

The purpose of this policy is to provide guidance to Pacific Gateway Workforce Innovation Network (Pacific Gateway) staff, subrecipients and America's Job Center of California (AJCC) partners on compliance with the requirements of handling and protecting personally identifiable information (PII).

BACKGROUND

As part of the grant activities, Pacific Gateway Workforce Innovation and Opportunity (WIOA) programs and other programs administered and/or overseen by Pacific Gateway (including AJCC partners), may have in their possession large quantities of personal and confidential information relating to their organization and staff, subrecipient 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. All parties are required to take aggressive measures to mitigate the risks associated with the collection, storage, and dissemination of PII.

POLICY AND PROCEDURES

A. Definitions

For purposes of this policy, the following are definitions of terms related to PII.

PII – the Office of Management and Budget (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 (DOL) has defined two types of PII, protected PII and non-sensitive PII. The differences are primarily based on an analysis regarding the "risk of harm" that could result from the release of 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 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. Essentially, it is stand-alone that is not linked or closely associated with any protected or unprotected PII. Examples of non-sensitive information 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. For example, 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 card number, a date of birth, and mother's maiden name could result in identity theft.

B. Requirements

Federal regulations require that PII and other sensitive information be protected. All Pacific Gateway staff, subrecipients, and AJCC partners must secure transmission of PII and sensitive data developed, obtained, or otherwise associated with WIOA funds or other funds administered or overseen by Pacific Gateway and must comply with the following:

- Ensure PII is not transmitted to unauthorized users and all PII and other sensitive data transmitted via email 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 all PII data on personally owned equipment, at off-site locations (i.e. employee's home, personal email) is strictly prohibited unless approved by Pacific Gateway's Workforce Development Board.

- Ensure all employees, subrecipients and AJCC partners who will have access to sensitive confidential, proprietary, and/or private data (1) are 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, subrecipients and AJCC partners 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 CalJOBS system for any purpose not stated in the grant or agreement with Pacific Gateway.

- Access to any PII data must be restricted to only those staff who need it in their official capacity to perform duties in connection with the scope of work in the grant or agreement with Pacific Gateway.

- 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 is encrypted.

- Must permit Pacific Gateway, federal and/or state staff to make onsite inspections during regular business hours for the purpose of conducting audits and/or other investigations to assure that staff, subrecipients and AJCC partners are 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, state and local records retention requirements, if any. Thereafter, all data must 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 is stays protected. Pacific Gateway staff, subrecipients and AJCC partners 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 steps that should be taken to protect PII:

    - Before collecting PII or sensitive information from participants, have participants sign Pacific Gateway's "Information Release and Privacy Statement" form 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 should 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. If SSNs are to be used for tracking purposes, they must be stored or displaced in a way that is not attributable to a particular individual such as 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 to Pacific Gateway's Deputy Director.

REFERENCES

- Title 20 CFR, "WIOA Final Rule" Section 683.220
- Training and Employment Guidance Letter (TEGL) 39-11, "Guidance on the Handling and Protection of Personally Identifiable Information (PII)" (June 28,2012)

INQUIRIES

For questions or assistance related to this policy, please contact Pacific Gateway Workforce Innovation Network staff at (562) 570-3748.