



APPROVAL DATE:

10/8/2014

APPROVED BY:

Carl Dudley, WIB Chair

**COUNTY OF SAN LUIS OBISPO
DEPARTMENT OF SOCIAL SERVICES**

POLICY NO: 42-08

TO: Service Providers

FROM: Department of Social Services

EFFECTIVE: September 26, 2014

SUBJECT: Handling and Protection of Personally Identifiable Information (PII)

REFERENCES:

- Department of Labor Training and Employment Guidance Letter (TEGL) No. 39-11

PURPOSE:

The purpose of this Policy is to provide guidance to WIA service providers on compliance with the requirements of acquiring, handling, transmitting and protecting personally identifiable information (PII).

BACKGROUND:

As part of their grant activities, WIA service providers may have in their possession large quantities of PII relating to individual program participants. This information is generally found in participant case files, both paper and electronic. Service providers are required to take measures to mitigate the risks associated with the collection, storage, and dissemination of PII.

DEFINITIONS:

For purposes of this policy, 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 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*, on the other hand, is information that if disclosed, by itself, could not reasonably be expected to result in personal harm. Essentially, it is stand-alone 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.

POLICY:

Federal law, and OMB Guidance polices require that PII and other sensitive information be protected. To ensure compliance with Federal law and regulations, WIA service providers must secure the storage and transmission of PII and sensitive data developed, obtained, or otherwise associated with WIA funds.

In addition to the requirement above, all grantees 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 e-mail or stored on CDs, DVDs, thumb drives, etc., must be encrypted using a Federal Information Processing Standards (FIPS) 140-2 compliant and National Institute of Standards and Technology (NIST) validated cryptographic module.
(For more information on FIPS 140-2 standards and cryptographic modules, grantees should refer to FIPS PUB 140-2, located online at: <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>)

Service providers must not email unencrypted sensitive PII to any entity, including contractors.

- Service providers must take the steps necessary to ensure the privacy of all PII obtained from participants and/or other individuals and to protect such information

from unauthorized disclosure. Grantees must maintain such PII in accordance with this policy.

- Service providers shall ensure that any PII used during the performance of their grant has been obtained in conformity with this policy and applicable Federal and state laws governing the confidentiality of information.
- Service providers further acknowledge that all PII data obtained through their WIA grant 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 grantee issued equipment, managed information technology (IT) services, and designated locations approved by the Administrative Entity. Accessing, processing, and storing of WIA grant 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), is strictly prohibited.
- Service provider's employees and other personnel 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.
- Service providers must have policies and procedures in place under which grantee employees and other personnel, 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.
- Service providers must not extract information from data supplied for any purpose not stated in the grant agreement.
- Access to any PII created by the WIA 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. Data may be downloaded to, or maintained on, mobile or portable devices only if the data are encrypted using NIST validated software products based on FIPS 140-2 encryption. In addition, wage data may only be accessed from secure locations.

A service provider's failure to comply with these requirements, or any improper use or disclosure of PII for an unauthorized purpose may result in the termination or suspension of the grant, or the imposition of special conditions or restrictions, or such other actions as the Administrative Entity may deem necessary to protect the privacy of participants or the integrity of data.

PROCEDURE:

Protected PII is the most sensitive information encountered in the course of grant work, and it is important that it stays protected. Service providers 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.
- 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 is 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.
- 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 DSS as the Administrative Entity for the grant, who will report it to ETA Information Security at ETA.CSIRT@dol.gov, (202) 693-3444, and follow any instructions received from officials of the Department of Labor.

ACTION:

The Administrative Entity for the WIB and its service providers shall follow this policy. This policy shall remain in effect until such time that a revision is required.

INQUIRIES:

Inquiries should be addressed to wibadmin@co.slo.ca.us.