Workforce Alliance of the North Bay Policy #: 1005

Effective Date: 10/11/2018

PERSONALLY IDENTIFIABLE INFORMATION (PII)

PURPOSE

The purpose of this policy is to provide guidance to Workforce Alliance of the North Bay (Alliance) service providers on compliance with the requirements of acquiring, handling, transmitting, and protecting Personally Identifiable Information (PII).

SCOPE

Workforce Alliance of the North Bay Staff
Workforce Innovation and Opportunity Act Title I contracted Service Providers

RESPONSIBLE PARTY

Workforce Alliance of the North Bay
Regional Workforce Development Board

REFERENCES

- Workforce Innovation and Opportunity Act (WIOA)
- U.S. Department of Labor, Training and Employment Guidance Letter (TEGL) WIOA NO. 39-11
- Federal Information Processing Standards (FIPS) 140-2
- Office of Management and Budget (OMB) M-07-16

DEFINITIONS

Non-Sensitive PII - 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.

PII - Information that can be used to distinguish or trace and individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

Protected PII - 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.

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.

Service Provider - WIOA Title I contracted service providers for One-Stop Operator, and Adult, Dislocated Worker, and Youth Services, as well as any other contracted entity providing WIOA services.

POLICY

I. Federal Law and OMB policies require that PII and sensitive information be protected. To ensure compliance with Federal Law and Regulations, Alliance service providers must secure the storage and transmission of PII and sensitive data developed, obtained, or otherwise associated with Workforce Innovation and Opportunities Act (WIOA) funds.

II. In addition to the requirement above, all grantees must also comply with all the following:

A. 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 Federal Information Processing Standards (FIPS) 140-2 compliant and National Institute of Standards and Technology (NIST) validated cryptographic module. **Service providers must not e-mail unencrypted sensitive or protected PII to any entity.**

B. 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 confidentiality of information.

C. Service providers further acknowledge that all PII data obtained through the provision of WIOA services 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 Alliance. Accessing, processing, and storing of WIOA 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.

D. Service providers' 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.

E. Service providers must have policies and procedures in place under which their 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 sanction for improper disclosure.

F. Service providers must not extract information from data supplied for any purpose not stated in the related Memorandum of Understanding (MOU), contracts, and/or agreements.

G. Access to any PII created by the WIOA grant must be restricted to only those employees of the service provider who need it in their official capacity to perform duties in connection with the scope of work in related MOU, contracts, and/or agreements.

H. 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.

I. Service providers must permit the Alliance to make onsite inspections during regular business hours for the purpose of conducting audits and/or conducting other investigations to assure compliance with the confidentiality requirements. In accordance with this responsibility, services providers must make records available to authorized persons for the purpose of inspection, review, and/or audit.

III. 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 termination or suspension of the WIOA grant, or the imposition of special conditions or restrictions, or such other actions as the Alliance may deem necessary to protect the privacy of participants or the integrity of data.

IV. Protected PII is the most sensitive information encountered by service providers and it is important to protect this information. Service Providers are required to protect PII and sensitive information when transmitting, collecting, transporting, storing, and/or disposing of information as well. Outlined below are steps to be followed to help protect PII:

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

B. Whenever possible, use unique identifiers for participant tracking instead of SSNs. When tracking individuals using an SSN, a truncated version should be used so that the full SSN does not display (***-**-1111 for example).

C. When disposing of paper files containing PII, the documents shall be shredded. Any PII stored electronically shall be deleted using a secure manner.

D. Records containing PII shall never be left unattended and computer terminals shall be password protected when a computer is left unattended for any length of time.

E. Documents containing PII shall be locked in cabinets when not in use and at the end of each business day.

F. When transporting documents containing PII, the documents shall be secured in a locked mobile file storage box/case.

V. Any perceived or suspected breach of PII either electronically or by other means shall be reported immediately to the Alliance Operations Analyst, who will report it to the US Department of Labor Employment and Training Administration (ETA) Information Security at ETA.CSIRT@dol.gov, (202) 693-3444.

POLICY UPDATE HISTORY

October 11, 2018 – New Policy

INQUIRIES

Questions regarding this policy can be sent to the Alliance Operations Analyst.