Operational Policy NO. OP - 432

Subject: Personally Identifiable Information (PII) Policy
Effective: PY17 - 7/1/2017

BACKGROUND

As part of their grant activities, Employment and Training Administration (ETA) Grantees may have in their possession large quantities of Personally Identifiable Information (PII) relating to their organization and staff; sub-grantee 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.

Federal agencies are required to take aggressive measure to mitigate the risks associated with the collection, storage, and dissemination of sensitive date including PII. ETA's Training and Employment Guidance Letter (TEGL No. 39-11) specifies requirements grantees must follow pertaining to the acquisition handling, and transmission of PII.

Definitions

- PII - 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 U.S. 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.

    - 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.
    - 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 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.

Policy

Federal law, OMB Guidance, U.S. Department of Labor and ETA polices require that PII and other sensitive information be protected. ETA has examined the ways its grantees, as stewards of Federal funds, handle PII and sensitive information and has determined that to ensure ETA compliance with Federal law and regulations, grantees must secure transmission of PII and sensitive data developed, obtained, or otherwise associated with ETA funded grants.

In addition to the requirement above, all grantees and sub-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. Grantees and Sub-grantees must not e-mail unencrypted sensitive PII to any entity, including ETA or contractors.

- Grantees and Sub-grantees 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 and Sub-grantees must maintain such PII in accordance with the ETA standards for information security described in TEGL No. 39-11 and any updates to such standards provided to the grantee by ETA.

- Grantees and Sub-grantees shall ensure that any PII used during the performance of their grant has been obtained in conformity with applicable Federal and state laws governing the confidentiality of information.

- Grantees and Sub-grantees further acknowledge that all PII data obtained through their ETA 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 ETA. Accessing, processing, and storing of ETA 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 unless approved by ETA.

- Grantee and Sub-grantee 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.

- Grantee and Sub-grantees must have their policies and procedures in place before Grantee and Sub-grantee staff are granted access to PII, acknowledge of 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.

- Grantees and Sub-grantees must not extract information from data supplied by ETA for any purpose not stated in the grant agreement.

- Access to any PII created by the ETA grant must be restricted to only those employees of the Grant Recipient and Sub-grantees 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.

- PII data obtained by the Grantee through a request from ETA must not be disclosed to anyone but the individual requestor except as permitted by the ETA Grant Officer.

- Grantees and Sub-grantees must permit ETA to make onsite inspections during regular business hours for the purpose of conducting audits and/or conducting other investigations to assure that the Grantee and Sub-grantees is complying with the confidentiality requirements described above. In accordance with this

responsibility, Grantee and Sub-grantees must make records available to authorized persons for the purpose of inspection, review, and/or audit.

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

A Grantee and Sub-grantees failure to comply with the requirements identified in TEGL No. 39-11, or any improper use or disclosure of PII for an unauthorized purpose, may result in the termination or suspension of the grant or sub-grant, or the imposition of special conditions or restrictions, or such other actions as the USDOL Grant Officer may deem necessary to protect the privacy of participants or the integrity of data.

Additional Requirements

Grantees and Sub-grantees 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 additional requirements to protect PII:

- Participants must sign WCCNM Participant Agreement, acknowledging the use of PII for grant purposes only.

- SSNs will initially be required for performance tracking purposes; however, the WCCNM will then use the State ID in place of the SSN after eligibility is determined and all information is entered for tracking purposes.

- Shredding will be used for destroying sensitive PII in paper files, and IT will securely delete sensitive electronic PII.

- Records containing PII will not be left open or unattended by staff.

- Documents containing PII will be kept in locked cabinets when not in use.

- If a breach is made or suspected, report immediately to provider supervisor and WCCNM WIOA Program Manager at (505) 724-3629

APPLICABILITY

All WCCNM Service Providers.

INQUIRIES

WIOA Manager 505-724-3629