Southwest Corner Workforce Development Board
Personally Identifiable Information (PII) policy

Purpose

The Purpose of the Personally Identifiable Information (PII) policy is to provide guidance to program providers on compliance with the requirements of handling and protecting PII in their grants. Employment and Training Administration provides guidance on the handling and protection of PII in Training and Employment Guidance Letter (TEGL) Number 39-11 dated June 28, 2012. The Southwest Corner Workforce Development Board (SCWDB) adopts this policy for all administrative, program, and fiscal operations.

Background

As part of the day to day activities, SCWDB program providers may have in their possession large quantities of Personally Identifiable Information (PII) relating to their organization and staff; partner organization and staff; and individual program participants. This information is generally found in personnel files, participant data sets, performance reports, program evaluations, and contract files and other sources.

In order to mitigate the risks associated with the collection, measures must be in place in regard to collection, storage, and dissemination of sensitive data including PII. The SCWDB Procurement Policy lists a brief overview of Federal level efforts to protect PII. This policy provides specific requirements that Providers must follow pertaining to the acquisition, handling, and transmission of PII.

Definitions

Definitions of PII include any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information:

(i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or

(ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media.

Office of Management and Budget (OMB) M-07-16 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.

Examples of Personally Identifiable Information

Examples of Personally Identifiable Information most often collected include the following:

- First or last name
- Date of birth
- Country, City or state of residence
- Social Security Number
- Credit Card number
- Immunization history/ medical record
- Age
- Telephone numbers/cell number
- Email addresses
- Gender
- Race
- Criminal Record
- Family income statements

Requirements

Federal law and OMB Guidance and ETA policies require that PII and other sensitive information be protected. All Providers must comply with the following:

- If at all possible, PII should never be transmitted via email. All PII and other sensitive data transmitted via email or stored on laptops, CDs, thumb/jump drives, etc., must be encrypted using Federal Information Processing Standards. The Provider shall ensure that any and all PII used during the performance of their grant has been obtained in the conformity with applicable Federal and state laws governing the confidentiality information.
- Provider must take the necessary steps to ensure privacy of all PII obtained from participants and/or other individuals and to protect such information from unauthorized use. Have participants sign releases acknowledging the collection of PII data for grant purposes. Do not leave records containing PII open or unattended.
- All PII obtained data shall be stored in an area that is physically safe from access by unauthorized persons at all times. Store documents containing PII in locked cabinets when not in use.
- Access to any PII information must be restricted to only those employees who need to perform duties in connection with the scope of work.
- Whenever possible, the use of unique identifiers for participant tracking is recommended instead of Social Security Numbers (SSN). While the SSN may initially be required for performance tracking proposes, a unique identifier should be linked to each individual record.
- PII data must not be disclosed to anyone but the individual requestor except as permitted by the SCWDB.

- Providers must permit SCWDB Monitors to allow onsite inspections for the purpose of conducting audits or other investigations to assure the Provider is complying with confidentiality requirements.

Provider's failure to comply with requirements identified in TEGL 39-11, or any improper use or disclosure of PII for an unauthorized use may result in the termination or suspension of the funding. Special conditions may be deemed necessary to protect the privacy of participants or integrity of the data.

Inquiries/Authorization Regulations

Providers will not disclose PII to anyone until management has verified the identity of the person requesting the information and the authority of that person to have access to it. A Disclosure Log must be maintained which will include: date of disclosure; name and address of the person who received the PII; a brief description of the PII disclosed and why the PII was disclosed.

Instance when an authorization to release PII may occur:

- Public Health Activities
- Health Oversight Activities
- Subpoenas and Court Orders
- Law Enforcement
- Reporting abuse, neglect or domestic violence cases
- Armed Services
- Averting serious threat to Health and Safety
- Federal or state audits of files.

Common Recommendations for Providers

Do not disclose, discuss or share participant's PII unless it is authorized. Provide a Notice of Privacy Practices to all participants.

Immediately report any breach of PII information to the Southwest Corner Workforce Development Board at rlaick@washingtongreene.org or by calling 724-229-5083 to discuss with WDB Management.