Title: Handling and Protection of Personally Identifiable Information
Date: Approved by the Workforce Alliance Board March 09, 2016

Handling and Protection of Personally Identifiable Information

Federal law, OMB Guidance, and Departmental and Employment and Training Administration (ETA) policies requires that Personally Identifiable Information (PII) and other sensitive information be protected. To ensure compliance with Federal law and regulations, the Workforce Alliance (WA), employees, and contractors must secure transmission of PII and sensitive data.

Employees and contractors must ensure that PII is not transmitted to unauthorized users, all PII and other sensitive data transmitted via email 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. Employees and contractors must not email unencrypted sensitive PII to any entity, including ETA or contractors.

Staff and contractors 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. Employees and contractors shall ensure that any PII used has been obtained in conformity with applicable Federal and state law governing the confidentiality of information.

Employees and contractors must acknowledge that all PII data obtained 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 issued equipment, managed information technology (IT) services, and designated locations approved by the WA. Accessing, processing, and storing of PII data on personally owned equipment, at off-site locations e.g. employee's home, and non-WA managed IT services, e.g. Yahoo mail, is strictly prohibited unless expressly approved by the WA.

Employees and other personnel who will have access to sensitive/confidential/proprietary/private data will 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.

Employees and other personnel, before being granted access to PII, should acknowledge their understanding of the confidential nature of the data and safeguards with which they must comply in their handling of such data as well as the fact that there may be liable to civil and criminal sanctions for improper disclosure.

Access to PII must be restricted to only those employees who need it in their official capacity to perform duties in connection with their work.

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.

The WA will allow onsite inspections during regular business hours for the purpose of conducting audits and/or conducting investigations to assure compliance with confidentiality requirements described in this policy. The WA will make records available to authorized persons for the purpose of inspections, review, and/or audit.

The WA will retain data only for the period of time required to use it for assessment and other purposes, or to satisfy applicable Federal records retention requirements. Thereafter, all data will be destroyed, including the degaussing of magnetic tape files and deletion of electronic data.

It is required to protect PII when transmitting information, but it is also required that PII and other sensitive information be protected when collecting, storing, and/or disposing of information as well.

Unique identifiers should be used for participant tracking instead of social security numbers. Appropriate methods for destroying PII in paper files should be used (i.e. shredding or using a burn bag) and sensitive electronic PII must be securely deleted. Records containing PII should not be left open and unattended. Documents containing PII should be stored in locked areas when not in use.

Any breach or suspected breach of PII should be reported immediately to management.

Definitions

Personally Identifiable Information (PII) is any information that can be used to distinguish or trace an individual's identity; either alone or in connection with other personal or identifying information that is linked or linkable to a specific individual

Sensitive Information is any unclassified information whose loss, misuse, or unauthorized access to or modification of could adversely affect the interest or the conduct of programs, or the privacy to which individuals are entitled under the Privacy Act.

Protected Personally Identifiable Information (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, 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, email 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.