Subject: Personally Identifiable Information (PII) Policy

Purpose: To transmit Coastal Counties Workforce Board's policy on PII

Statutory Authority: Privacy Act 5 U.S.C. 555; MDOL, MDOL, BES PL15-10.

Effective Date: September 10, 2015

Revision Date(s): December 14, 2023

Expiration Date: Indefinite

Personally Identifiable Information (PII) and Sensitive Information Policy Statement

As a general practice, Coastal Counties Workforce, Inc. does not obtain or hold personally identifiable information; solely the service provider preserves such information. However, in the event that information is shared and/or stored in CCWI offices, all rules/guidance as outlined in TEGL No. 39-11 will be applied as appropriate.

Per TEGL 39-11, PII is defined "as information that can be used to distinguish or trace an individual's identify, either alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual."[1]

Sensitive Information is defined as "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."[2]

TEGL 39-11 defines two types of PII, protected PII and non-sensitive PII. According to TEGL 39-11, the differences between the two are primarily based on an analysis regarding the "risk of harm" that could result from the release of PII.

- Protected PII is information that if disclosed could result in harm to the individual whose name or identity is linked to that information. This includes (but is not limited to): social security numbers, credit card and bank account numbers, home telephone numbers, ages,

[1] U.S. Department of Labor. Employment and Training Administration Advisory System. Advisory: Training and Employment Guidance Letter No. 30-11. Washington D.C. (June 28, 2012), https://www.dol.gov/agencies/eta/advisories/training-and-employment-guidance-letter-no-39-11.

[2] Ibid.

birthdates, marital status and spouse names, educational history, biometric identifiers (fingerprints, voiceprints etc), medical history, financial information and computer passwords.

- Non-sensitive PII is information if disclosed, by itself, could not be reasonably be expected to result in personal harm---standalone information that is not linked or closely associated with any protected or unprotected PII. For example, first and last names, email and business addresses, business telephone numbers, general education credentials, gender or race.

  NOTE: Depending on the circumstances, a combination of these items could potentially be considered protected or sensitive PII: By way of example, a name linked to a social security number, date of birth and mother's maiden name could result in identity theft. This illustrates why protecting the information of our clients is so important.

For CCWI, the service provider, and its staff, in any instance when PII or sensitive information is obtained the receiver will ensure compliance with Federal law and regulations and the following provisions shall apply:

- All PII used during the performance of the grant has been obtained in conformity with applicable Federal and state laws governing the confidentiality of information and will be protected from unauthorized disclosure.
-
- All policies and procedures are in place under which all employees acknowledge their understanding of the confidential nature of the data and the safeguards with which they must comply
- Staff will not extract information for any purpose not stated in the grant agreement
- Any PII created by the grant must be restricted to only those employees who need it in their official capacity to perform duties in connection with the scope of work in the grant agreement
- PII data requested by ETA must not be disclosed to anyone but the individual requestor except as permitted by the Grant Officer
- ETA and Maine Department of Labor (MDOL), as applicable, will be allowed to make onsite inspections during regular business hours for the purpose of conducting other investigations to assure that CCWI and the service provider is complying with confidentiality requirements
- CCWI will 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

Additionally, the service provider and its staff will adhere to the following provisions:

- 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. The service provider will not e-mail unencrypted sensitive PII to any entity

- 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 service provider issued equipment, managed information technology (IT) services, and designated locations approved by CCWI. Accessing, processing, and storing of ETA grant PII data on personally owned equipment, at off-site locations e.g., employee's home, and non-service provider managed IT services, e.g., Yahoo mail, is strictly prohibited unless approved by the ETA.
- All employees will be advised of the confidential nature of the information, the safeguards required to protect the information, and that there are civil sanctions for noncompliance with such safeguards that are contained in Federal and state laws
  All PII will 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 devises 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 a secure location.

Grantees (or subgrantees) that fail to comply with these requirements, or that have improperly disclosed or utilized PII information for an unauthorized purpose are at risk of termination or suspension of their grant and imposition of special conditions or restrictions as deemed necessary to protect the privacy of the participants or the integrity of data.

Confidentiality:

In order to maintain public confidence and trust, CCWI and the service provider shall require each staff member to sign an affirmation of their understanding of the policy and assurance that they:

- Will not, except as necessary in the normal course of business, divulge employer, claimant, customer, participant, or co-worker information obtained in the performance of their official duties to any person within or outside of the agency unless specifically authorized to do;
- Will not obtain information through agency computers, documents, or other official means for any purpose other than official business;
- Will not duplicate, alter, use or disclose any information obtained through such systems or documents without proper authorization;
- Will not, except as necessary in the normal course of business, remove documents, property or equipment containing sensitive information from the workplace under any circumstances, unless authorized to do so;
- Will not access personal information maintained by the agency pertaining to his/her relatives, neighbors, or any other individuals that staff person is not authorized to access as part of his/her regular duties;
- Will not disclose agency computer security codes, passwords, or combinations thereof to the public, friends, relatives or co-workers;
- Will not trace, attempt to duplicate or otherwise forge a claimant, employer, customer, participant, vendor or co-worker signature on any document.

Custody of PII Records:

Federal law requires that Personally Identifiable Information and other sensitive information be protected during the collection, storage and disposal processes. Before collecting PII or sensitive information from participants or agencies with information about participants, ensure that signed releases acknowledging the use of the specific PII is only for grant purposes.

Always use a unique identifier when referencing a participant instead of SSNs. While SSNs may initially be required for performance tracking purposes, a unique identifier must be linked to each individual record. Once the SSN is entered for performance tracking purposes the unique identifier must be used in place of the SSN for tracking purposes. SSNs 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 by shredding or depositing in a secure shredding bin and securely delete sensitive electronic PII using special software designed to do so.

Never leave records containing PII open and unattended, ensure that paper records are locked away in file cabinets and ensure that your work PC locks every so many minutes and that it requires a secure passcode to unlock it.

Ensure that passcodes are complex enough that they cannot be guessed by potential hackers.

Ensure that computer passwords are secure and never share passwords with anyone (not even your supervisor or co-worker).

Breach of PII

Any breach of PII must be reported immediately to the Federal Program Officer responsible for the grant, to ETA Information Security at ETA.CSIRT@dol.gov or at (202) 693-3444 and follow any instructions received from officials of the Department of Labor (DOL). Also contact Maine Department of Labor (MDOL). Use MDOL protocols in place to inform and protect affected participants/employees should a breach occur, so long as those protocols do not conflict with DOL instructions.

In the event of a fire or natural disaster (flood, storm, earthquake), the service provider must have a written plan in place in place pertaining to file recovery or proper file destruction.

Staff Training

The service provider must ensure that all staff receives awareness training of the requirements pertaining to confidentiality and access, handling and protection of PII; of the consequences of breach of or misuse of PII and the requirement to sign a statement acknowledging their understanding of these requirements.

LWIB Approved: __12/14/2023__