Title: Personally Identifiable Information Policy	**Date of Issue:** 07/01/2021
Approved By: Heather Powell	**Last Reviewed: 01/12/2026**

BACKGROUND:

Carroll County Workforce Development (CCWD) may have in their possession large quantities of Personally Identifiable Information (PII) relating to their organization and staff; partner organizations, subrecipients, 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.

This policy provides guidance to staff and subrecipients in compliance with the requirements of handling and protecting PII in accordance with federal and State of Maryland regulations, Uniform Guidance, and US Department of Labor TEGL 39-11.

DEFINITIONS:

A. Uniform Guidance 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.

B. 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 Federal programs, or the privacy to which individuals are entitled under the Privacy Act.

C. Protected PII and non-sensitive PII - the Department of Labor (the Department) 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.

1. 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.

2. Non-sensitive PII, on the other hand, 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.

D. 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 CCWD program participants is so important.

POLICY:

A. Federal law, Uniform Guidance, Carroll County Department of Economic Development and ETA polices require that PII and other sensitive information be protected.

B. All CCWD staff, partners and subrecipients must also comply with all of the following:

1. To ensure that such PII is not transmitted to unauthorized users, all PII and other sensitive data transmitted via e-mail or stored 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 (Refer to FIPS PUB 140-3). Staff and subrecipients must not e-mail unencrypted sensitive PII to any entity.

2. CCWD staff, partners and subrecipients 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. CCWD staff, partners and subrecipients must maintain such PII in accordance with the standards for information security described in TEGL 39-11 and any updates to such standards provided by ETA.

3. CCWD staff, partners and subrecipients shall ensure that any PII used during the performance of their grant/contract has been obtained in conformity with applicable Federal and state laws governing the confidentiality of information.

4. CCWD staff, partners and subrecipients further acknowledge that all PII data obtained through their grant/contract 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 staff or subrecipient issued equipment, managed information technology (IT) services, and designated locations. Accessing, processing, and storing of PII data on personally owned equipment, at off-site locations e.g., employee's home, or non-subrecipient managed IT services, e.g., personal mail, is strictly prohibited.

5. CCWD staff, partners and subrecipient employees 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.

6. Subrecipients must have their policies and procedures in place under which CCWD 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 sanctions for improper disclosure.

7. Access to any PII must be restricted to only those CCWD staff, partners and subrecipient employees who need it in their official capacity to perform duties in connection with the scope of work in the grant/contract agreement.

8. 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 PUB 140-3 encryption. In addition, wage data may only be accessed from secure locations.

9. CCWD staff and subrecipients must permit ETA or MDOL to make onsite inspections during regular business hours for the purpose of conducting audits and/or conducting other investigations to assure that the grantee is complying with the confidentiality requirements described above. In accordance with this responsibility, staff and subrecipients must make records available to authorized persons for the purpose of inspection, review, and/or audit.

10. CCWD staff and subrecipients 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. Afterwards, all data will be destroyed and deletion of electronic data.

C. Staff's failure to comply with the requirements identified in TEGL 39-11, or any improper use or disclosure of PII for an unauthorized purpose, may result in disciplinary action.

D. Subrecipients failure to comply with the requirements identified in TEGL 39-11, or any improper use or disclosure of PII for an unauthorized purpose, may result in the termination or suspension of the contract, or the imposition of special conditions or restrictions, or such other actions as the CCWD may deem necessary to protect the privacy of participants or the integrity of data.

E. Recommendations:

1. Protected PII is the most sensitive information that you may encounter in the course of your work, and it is important that it stays protected. CCWD staff, partners and subrecipients 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.

2. Outlined below are some recommendations to help protect PII:

   a. Before collecting PII or sensitive information from participants, have participants sign releases acknowledging the use of PII for grant/contract purposes only.

   b. Whenever possible, ETA recommends the use of unique identifiers for participant tracking instead of SSNs. While SSNs may initially be required for performance tracking purposes, a unique identifier could be linked to each individual record. Once the SSN is entered for performance tracking, the unique identifier would be used in place of the SSN for tracking purposes. If SSNs are to be used for tracking purposes, they must be stored or displayed in a way that is not attributable to a particular individual, such as using a truncated SSN.

   c. Use appropriate methods for destroying sensitive PII in paper files (i.e.shredding) and securely deleting sensitive electronic PII.

   d. Do not leave records containing PII open and unattended.

   e. Store documents containing PII in locked cabinets when not in use.

   f. Immediately report any breach or suspected breach of PII to the CCWD.

   g. The CCWD will report any breach or suspected breach of PII to the awarding agency.

REFERENCES:

Public Law 113-128
TEGL 39-11
FIPS PUB 140-3

WEBSITE: https://carrollworks.com/