

---

---


EMPLOYERS' TRAINING RESOURCE

1600 E. Belle Terrace

Bakersfield, CA 93307

**POLICY BULLETIN: #ETR 25b-21**

TO: All ETR Staff and Service Providers

FROM:  Teresa Hitchcock  
Assistant County Administrative Officer

DATE: August 5, 2021

SUBJECT: Handling and Protection of Personally Identifiable Information (PII)

**This Policy Bulletin Supersedes Any Previously Issued Policy Statements  
Concerning Personal and Confidential Information Policies and Procedures**

---

**PURPOSE:**

The purpose of this policy is to communicate requirements for the security of personal and confidential information Employers' Training Resource (ETR) staff and service providers receive from individuals applying for or receiving services as participants through the Workforce Innovation and Opportunity Act (WIOA) or other funding sources.

**BACKGROUND:**

As WIOA or other funded sources are provided through a customer-centered case management system, staff obtain personal and confidential information from individuals to the extent allowed by state and federal law in order to facilitate an individual's access to service.

ETR and its service providers have in their possession large quantities of PII relating to their organization and staff; partner organizations and staff; and individual program participants.

**DEFINITIONS:**

- Service Providers – For the purpose of this policy, Service Providers include ETR subrecipients ***including agencies contracted to work with employers who provide Work Experience,*** America's Job Center of California (AJCC) partners, Eligible Training Provider List (ETPL) training providers, ETR staff, and ***employers or host employers providing On-The-Job Training, Incumbent Worker Training, or Transitional Jobs Training.***
- PII – 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 United States Department of Labor (DOL) has defined two types of PII: (1) Protected PII and (2) Non-sensitive PII. The differences between the protected PII and non-sensitive PII are primarily based on an analysis regarding the “risk of harm” that could result from the release of PII. (TEGL 39-11)
  - (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 name, educational history, biometric identifiers (fingerprints, etc.), medical history, financial history, 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, 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.

## **POLICY:**

Federal law, OMB Guidance, and DOL policies require that PII and other sensitive information be protected. To ensure compliance with Federal law and regulations, ETR service providers must secure the storage and transmission of PII and sensitive data developed, obtained, or otherwise associated with WIOA funds and must 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 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.
- Service providers 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. Service providers must maintain such PII in accordance with this policy.
- Service providers shall ensure that any PII used during the performance of activities associated with ETR have been obtained in conformity with this policy and applicable Federal and state laws governing the confidentiality of information.

- Service providers further acknowledge that all PII data obtained through their association with ETR shall be stored in an area that is physically safe from access by unauthorized persons at all times.
- Service provider's employees and other personnel who will have access to sensitive, confidential, proprietary, or 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.
- Service providers must not extract information from data supplied by the CalJOBS or any other participant-tracking system used in the course of work with ETR for any purpose not stated in their agreement with ETR.
- Access to any PII 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 their agreement with ETR.
- 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.
- Service providers must permit county, state, and federal staff to make onsite inspections during regular business hours for the purpose of conducting audits and/or conducting other investigations to assure that the service provider is complying with the confidentiality requirements described in this policy.
- Service providers must retain data only for the period of time required to use it for assessment and other purposes, or to satisfy applicable Federal records requirements, if any. Thereafter, all data will be destroyed, including the degaussing of magnetic tape files and deletion of electronic data.

## **PROCEDURE:**

Protected PII is the most sensitive information encountered in the course of grant work, and it is important that it stays protected. Service providers 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. In order to help protect PII, service providers shall comply with the following:

- Immediately report any breach or suspected breach of PII to ETR as the Administrative Entity for the grant, who will report it to ETA Information Security at [ETA.CSIRT@dol.gov](mailto:ETA.CSIRT@dol.gov), (202) 693-3444, and follow any instructions received from officials of the Department of Labor.
- Before collecting PII or sensitive information from participants, service providers must have participants sign and date the "Authorization to Share Confidential Information and Records" form (copy attached).
- Whenever possible, use unique identifiers, such as case numbers, for participant tracking instead of SSNs. While SSNs are initially required for performance tracking purposes, a unique identifier

should be used in place of SSN for participant tracking purposes. If SSNs must 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.

- Avoid communicating PII or sensitive information about an applicant/participant via email or personal cell phone. Further, participant information must only be communicated through agency approved email addresses and not through third party or personal email addresses such as Hotmail, Yahoo, etc.
- Use appropriate methods for destroying sensitive PII in paper files (i.e., shredding or using a burn bag) and securely deleting sensitive electronic PII.
- Do not leave records containing PII open and unattended. This includes copies or print jobs left unattended in copy machines or printers.
- Store documents containing PII in locked cabinets when not in use.
- Be discreet when verbally communicating personal and confidential information and ensure the receiver(s) are authorized to receive the information.
- Personal and confidential information that contains health information related to a physical or mental disability, medical diagnosis, or perception of a disability related to the individual, must be treated as confidential, collected on separate forms, and kept in a separate locked file apart from working files. Electronic files must be secured through password protection.

Any medical information contained in case notes must be redacted from the participant file; the original notes must be placed in the participant's medical file.

To minimize the need for staff to access a medical file, only the portion of the participant's information that reveals the presence of a disability should be included in the medical file.

**Access to the medical files:**

- Must be limited and should only be accessed with the approval of program management and when such access is necessary to facilitate a participant's access to services or to support an ongoing service plan; or
- First aid and safety personnel may be provided participant medical information in the event of an emergency; or
- Local, state or federal monitors, in compliance with 29 CFR Part 32.44(c) and 29 CFR Part 38.60, may have access to medical files for monitoring purposes.

**ACTION REQUIRED:**

Service providers are required to take aggressive measures to mitigate the risks associated with the collection, storage, and dissemination of sensitive data including PII.

A service provider's failure to comply with the requirements identified in this directive, or any improper use or disclosure of PII for an unauthorized purpose, may result in the termination or suspension of the agreement with ETR, or the imposition of special conditions or restrictions, or such other actions as ETR may deem necessary to protect the privacy of participants or the integrity of data.

**REFERENCES:**

- TEGL 39-11 - Guidance on the Handling and Protection of Personally Identifiable Information (PII)
- 20 CFR 680.110 – Workforce Innovation and Opportunity Act; Final Rule
- 2 CFR 200.303(e) – Office of Management and Budget Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards; Final Rule
- Employment Development Department Directive WSD17-01 – Nondiscrimination and Equal Opportunity Procedure

## AUTHORIZATION TO SHARE CONFIDENTIAL INFORMATION AND RECORDS

### PURPOSE OF THIS FORM

The purpose of this form is to obtain your permission to share your confidential information and records, including your social security number, among the partner agencies and/or service providers of the Kern, Inyo, and Mono Counties America's Job Center of California (KIM AJCC). By sharing your confidential information and records, the partner agencies and service providers of the KIM AJCC will be able to better assist you in identifying and accessing employment, training, and educational services.

### PLEASE READ THE FOLLOWING CAREFULLY

I understand that the partner agencies of the KIM AJCC system are requesting my permission to share my confidential information and records in order to facilitate access to programs under the United States Workforce Innovation and Opportunity Act (WIOA), Public Law 113-128, July 22, 2014.

I understand that I am not required to give permission to share my confidential information and records, including social security number, among the partner agencies of the KIM AJCC system.

I understand that if I agree to share my confidential information and records, including my social security number, the information will be shared solely with members of the partner agencies of the KIM AJCC system and for the sole purposes of enabling members of the KIM AJCC system to provide me employment and training services.

I understand that if I do not agree to share my confidential information and records, that information, and those records, will only be shared to the extent allowed by Federal and state law.

I understand that my eligibility to participate in KIM AJCC programs does not depend on my agreement to share my confidential information and records including my social security number. In fact, if I request that private and confidential information not be shared among the partner agencies of the KIM AJCC system, my eligibility for services will not be affected.

I understand that my confidential information and records may contain information regarding medical diagnosis or treatment for drug or alcohol abuse (42 CFR, Part 2).

☐ **I consent and agree to share my records:**

I, (Print Name) \_\_\_\_\_ hereby consent and agree that the partner agencies of the KIM AJCC system may share my confidential information and records including, but not limited to my: name; address; telephone number; email address; social security number; date of birth; age; educational records; as described in the Family Education Rights and Privacy Act of 1974, 20 USC 1232g; gender; race/ethnicity; employment history (e.g.: employer name, wages, work hours, etc.); financial information (such as household income and student financial aid information, including award status and amounts); and my eligibility for special programs (e.g.: disability, veteran, dislocated worker, economically disadvantaged, public assistance, food stamps, or unemployment insurance programs).

Or,

☐ **I do not consent to share my records:**

I, (Print Name) \_\_\_\_\_ do not agree to share my confidential information and records with the partner agencies of the KIM AJCC system.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

Signed copy must be placed in participant file at the time of enrollment into the WIOA Program  
Effective July 1, 2018