Sacramento
Employment and
Training
Agency

D'et Saurbourne
Interim Executive Director

925 Del Paso Blvd., Suite 100
Sacramento, CA 95815

Main Office
(916) 263-3800

Head Start
(916) 263-3804

Website: http://www.seta.net

September 25, 2023

To: All SETA Workforce Development Department Staff, Subgrantees and Partners

From: D'et Saurbourne, Interim Executive Director

RE: SAFEGUARDING CONFIDENTIAL AND PERSONALLY IDENTIFIABLE INFORMATION (PII) **#WDD 23-01**

Background

The Privacy Act of 1974 safeguards individuals against invasions of privacy when sensitive information is required for official use. SETA may have large quantities of sensitive information relating to the organization, staff, subrecipients, partner organizations, and individual program participants by virtue of its status as a steward of federal funding. This information is generally found in personnel files, participant data sets, performance reports, program evaluations, contract files, and other sources.

The Workforce Innovation and Opportunity Act (WIOA) requires that all sensitive information:

- Is collected, used, and stored in a manner that ensures it will not be accessible to anyone not authorized to access it;
- Is not collected unless needed for the provision of some service or to determine eligibility for a program;
- Is not used for any purpose other than the program or service for which it was collected, unless the subject of the information (if the subject is an adult), or a parent of the subject (if the subject is a minor or dependent), provides consent for the information to be shared;
- Can be released to the subject of the information upon his or her request;
- Is not accessible to anyone other than those authorized to access it (including agents of oversight and regulatory entities, and in cases in which the information has been subpoenaed, parties to the legal matter); and
- Is published only in aggregate form, preventing readers from being able to identify, or reasonably infer the identity of, any individual subject.

References

- The Privacy Act of 1974 (Public Law 93-579)
- WIOA (Public Law 113-128) Section 188
- TEGL No. 5-08
- TEGL No. 39-11
- OMB Memorandum M-07-16
- 2 CFR Part 200.79 & 200.82
- 29 CFR Section 38

- EN RFQ-12-0010L 8-27-12
- WSD 17-01

Local Policy

SETA's policy is to make every reasonable effort to safeguard confidential information, including personally identifiable information (PII). All staff and subrecipients shall strictly adhere to state and federal regulations pertaining to privacy, confidentiality, and record security.

Consistent with U.S. Department of Labor guidelines, this policy advises all staff, subgrantees, and partners who have access to sensitive/confidential/proprietary/private data, 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. In addition, before being granted access to PII, all staff, subgrantees, and partners must 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. Confirmation of the receipt of this policy via email constitutes such an acknowledgement by staff, subgrantees, and partners.

In addition to the minimum requirements outlined above, SETA shall:

- Assign pseudo social security numbers to program participants upon request;
- Utilize appropriate computer, network, and internet security controls;
- Dispose of confidential information and PII in a safe and secure manner; and
- Follow the Social Security Administration's (SSA's) safeguarding policy for beneficiaries' PII.

In addition, any medical or disability-related information obtained about a particular individual, including information that could lead to the disclosure of a disability, must be collected on separate forms. All such information, whether in hard copy, electronic, or both, must be maintained in one or more separate files, apart from any other information about the individual, and treated as confidential.

Whether these files are electronic or hard copy, they must be locked or otherwise secured (i.e., through password protection).

Pseudo Social Security Numbers

If an individual chooses to not provide his/her social security number, the individual shall not be denied services (if otherwise, eligible). While it is a requirement that each individual determined to be a program "participant" must be *requested* to provide his/her social security number in order to be included in the performance cohort, the individual is not required to disclose his/her social security number in order to be eligible to receive services.

In the case of an individual who chooses to not disclose his/her social security number staff shall assign a pseudo number for tracking purposes and shall follow-up with the individual to obtain supplemental data as verification of performance outcomes. Service providers may contact SETA's Systems Administrator for additional information on issuing pseudo numbers.

Handling and Record Security

Staff and subrecipients shall ensure personnel files, case files, and related records are not left unattended in work stations located in unsecured or public areas. Confidential information must be stored in a locked cabinet or secured area when not in use or under the direct control of authorized personnel.

Ticket to Work Program

As an approved Employment Network (EN), SETA shall protect Ticket Program beneficiaries' PII in accordance with Part III, Section 6 and Part IV, Section 3 of the EN agreement. SETA and its subrecipients shall:

- Use and access beneficiary information only for the purposes of SSA's Ticket Program;
- Dispose of beneficiary information in a safe and secure manner;
- Not duplicate or disseminate beneficiary information outside the EN's organization;
- Provide physical safeguards for protecting the security of beneficiary information, including restricting access only to authorized employees and officials who have received their security clearance and who need the information to perform their official duties in connection with SSA's Ticket Program;
- Store beneficiary information in a physically secure area and assure that it cannot be accessed and retrieved by unauthorized personnel; and
- Ensure that all personnel who have access to beneficiary information have met the security and suitability requirements and have complied with SSA's security awareness and Federal Information Security and Management Act (FISMA) training requirements.

Staff with limited access to Ticket Program beneficiary's PII solely through a beneficiary's self-disclosure of such information as part of the service delivery process would not need to complete the Social Security suitability process. Such staff would, however, need to follow the safeguarding strategies outlined above.

Instructions for Reporting Lost, Compromised, or Potentially Compromised PII

When an employee or subrecipient becomes aware or suspects that PII has been lost, compromised, or potentially compromised he/she shall provide **immediate** notification of the incident to SETA's Equal Opportunity Officer (EOO). The employee or subrecipient shall provide complete and accurate information including:

- A description of the loss, compromise, or potential compromise
- A description of the safeguards used (locked cabinet, redacted PII, password protection, etc.)
- Whether the employee or subrecipient has contacted or been contacted by any external organization (law enforcement, media, etc.)
- Whether or not the PII of Ticket Program beneficiaries was affected

In the event the loss, compromise, or potential compromise includes the PII of Ticket Program beneficiaries, additional reporting requirements apply (see Part IV, Section 3.K of the EN agreement). Finally, the employee or subrecipient shall limit disclosure of the details about an incident to only those with a need to know.