AB 24-02
Effective: Immediately upon release

ACTION BULLETIN

TO: All Alameda County Workforce Development Board (ACWDB) Career Service Providers (CSP) and Subcontractors supported through Workforce Innovation and Opportunity Act (WIOA) Title I Formula Funds (Youth, Adult, and Dislocated Worker) or through any discretionary or special project funds

DATE: January 24, 2024

SUBJECT: **Personal Identifiable Information (PII) Protection Policy**

PURPOSE OF THE BULLETIN:

The purpose of this bulletin is to provide guidance for ACWDB's Career Service Providers (CSP) and subcontractors to manage protections on the Personal Identifiable Information (PII) of publicly funded workforce program participants and applicants – and universal customers that are not enrolled in any publicly funded programs.

CITATIONS:

- Public Law 113-128 – Workforce Innovation and Opportunity Act of 2014
- U.S. Department of Labor (DOL), Employment and Training Administration (ETA) Training and Employment Guidance Letter (TEGL) 39-11; Issued 6/28/2012
- The Privacy Act of 1974
- U.S. Department of Commerce, National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS)
- NIST SP 800-122, Guide to Protecting the Confidentiality of PII
- Office of Management and Budget (OMB) Memorandum M-06-15, Safeguarding PII
- OMB Memorandum M-06-19, Reporting Incidents Involving PII
- OMB Memorandum M-07-16, Safeguarding Against and Responding to Breaches of PII
- Computer Security Act of 1987
- Federal Information Security Management Act (FISMA) of 2002

BACKGROUND:

This policy provides guidance regarding the handling and protection of individual PII. As part of their grant activities, ACWDB's subcontractors may have in their possession large quantities of PII relating to their organization and staff and individual program applicants and participants. All grantees (hereinafter referred to as service providers or subcontractors) with access to PII are required to take aggressive measures to mitigate the risks associated with the collection, storage, and dissemination of sensitive data including PII. This bulletin serves as notification of the specific requirements subcontractors must follow pertaining to the acquisition, handling, storage, and transmission of PII.

DEFINITIONS:

For the purposes of this bulletin, the following definitions apply:

PII: The Office of Management and Budget 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.

Sensitive Information: is any unclassified information whose loss, misuse, or unauthorized access to or modification of could adversely affect the interests or the conduct of programs, or the privacy to which individuals are entitled under the Privacy Act of 1974.

Protected PII vs non-sensitive PII: The DOL has defined two types of PII, protected PII and non-sensitive PII. The differences 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, (i.e., social security number, credit card information, bank account information, home telephone numbers, age, birthdate, fingerprints, medical history, financial information, and computer passwords).

2. Non-sensitive PII is information that if disclosed, by itself, could not reasonably be expected to result in personal harm. (i.e., first or last names, email addresses, business telephone numbers, gender, etc.). However, depending on the circumstances, a combination of these items could potentially be categorized as protected or sensitive PII.

REQUIREMENTS:

1. Federal law, OMB guidance, and departmental and ETA policies require that PII and other sensitive information be protected. ETA has determined that to ensure compliance with federal law and regulations, subcontractors must secure transmission of PII and sensitive data developed, obtained, or otherwise associated with ETA funded grants.

2. All PII and other sensitive data transmitted via email or stored on computer systems, DVDs, 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. Subcontractors must not email unencrypted sensitive PII to any entity, including funders or contractors.

3. Subcontractors must take all steps necessary to ensure the privacy of all PII obtained from participants and/or other individuals and to protect such information from unauthorized disclosure. Subcontractors must maintain PII in accordance with the ETA standards for information security described in this bulletin and any updates to such standards provided to the subcontractor by the ACWDB.

4. Subcontractors shall ensure that any PII used during the performance of their grant has been obtained in conformity with applicable federal, state, and local laws governing the confidentiality of information.

5. Subcontractors further acknowledge that all PII data obtained through any publicly funded grant 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 approved equipment, managed information technology (IT) services, and designated locations approved by the funder. Accessing, processing, and storing of PII data on personally owned equipment, at off-site locations, and through non-managed IT services is strictly prohibited unless approved by DOL.

6. Subcontractor 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, state, and local laws.

7. Subcontractors must have their policies and procedures in place and personnel with access to PII must understand and agree to comply with those policies and procedures in advance of being granted access to sensitive information. Such personnel must also understand the liability and/or civil or criminal sanctions for improper disclosure of PII.

8. Subcontractors and/or their employees must not extract information from sensitive or private data for any purpose other than those specifically required to carry-out responsibilities as outlined within the guidelines and in coordination with the performance of the publicly-funded program/grant.

9. Access to any PII created through the performance of duties related to the publicly-funded grant programs must be restricted to only those employees of the subcontractor who require it in their official capacity to perform duties in connection with the scope of work in the grant agreement.

10. 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. Wage data may only be accessed from secure locations.

11. PII data obtained by the subcontractor through a request from the funder must not be disclosed to any person other than the individual requestor except as permitted by the funder.

12. Subcontractors must permit ACWDB to make onsite inspections during regular business hours for the purpose of conducting audits and/or other investigations to assure compliance with the confidentiality requirements described in this bulletin. In accordance with this responsibility, subcontractors must make records as identified in this bulletin available to authorized persons for the purpose of inspection, review, and/or audit.

13. Subcontractors must retain data received from the funder only for the period required to use it for assessment or other purposes, or to satisfy applicable federal records retention requirements, if any. Thereafter, the subcontractor agrees that all data will be destroyed.

14. A subcontractor's failure to comply with the requirements identified in this bulletin, or improper use or disclosure of PII for an unauthorized purpose, may suffer termination or suspension of their grant, or the imposition of special conditions or restrictions, or such other action as the funder may deem necessary to protect the privacy of participants or the integrity of the data.

ACTIONS:

All ACWDB contracted service providers who administer programs within the community must adhere to policies and requirements as outlined in this bulletin. Additionally, upon release of this bulletin, service provider staff who view, handle, store or transmit an individual's PII must become familiar with this bulletin and must review, sign, and submit the Staff Confidentiality Agreement (Attachment 2 to this bulletin) to the attention of the ACWDB Program Liaison and the Workforce Services Technicians.

Protected PII is the most sensitive information that may be encountered while executing grant work, and it is important that it stays protected. Subcontractors are required to protect PII when transmitting information and required to protect PII and sensitive information when collecting, storing, and/or disposing of information as well. Outlined below are some recommendations to help protect PII:

A. Before collecting PII or sensitive information (i.e., Intake/screening forms, program applications, or copies of various forms of identification) from individuals, have them sign a release acknowledging the use of PII for grant purposes only.

B. Whenever possible, ETA recommends the use of unique identifiers for participant tracking instead of PII. While individual SSNs may be initially required for performance tracking purposes, a unique identifier could be linked to each individual record and used to track services and outcomes for individuals. The CalJOBS^{SM} system automatically generates unique identifiers (State ID numbers, and User ID numbers) for every individual who registers in that system. This auto-generated number could be used instead of SSNs.

C. Use appropriate methods for destroying sensitive PII (i.e., shredding) and securely delete sensitive electronic PII. Do not discard sensitive PII in standard trash bins.

D. Do not leave records containing PII open or unattended.

E. Store documents containing PII in locked cabinets or travel cases when not in use. This includes situations when travelling with PII.

F. Lock computer desktops or log out when leaving your desk area.

G. When transmitting PII data to ACWDB or other organizations, the data must be encrypted (reference Item #2 in the "Requirements" section above).

H. Immediately report any breach or suspected breach of PII to ACWDB and to ETA Information Security at ETA.CSIRT@dol.gov (202.693.3444) and follow any instructions received from the officials of the Department of Labor.

I. The CalJOBS^{SM} system offers a Document Management Module that would allow subcontractor and ACWDB Department staff to securely share PII and sensitive information and documentation with other organizations without having to email or physically transport the data. This module should be used as a secure method for transmitting and storing sensitive PII data.

File Retention Expectations: Case files for WIOA applicants and participants should be maintained for at least three program years (PY) beyond the exit date for that participant. [Example: If a WIOA participant exits WIOA program services during the first quarter of the PY (July, August, September of 2023), then the file should be maintained at least through the end of the third program year after the PY of exit (through at least July, 2027). However, each service provider may implement practices that call for a longer period of retention.
Case files containing references and/or documentation related to an individual's disability and/or any medical diagnosis must be maintained separately from the regular participant records – whether hard copy or electronic.

Any discrepancies arising between this policy/procedure and federal or state provisions (due to future revisions) will default to the current minimum federal and state regulations and guidance available. This bulletin represents the most current information available at the time it was published. As policies or regulations are updated, the most current versions of bulletins will appear on our website at www.acwdb.org.

Information and Inquiries:

For further information and inquiries please contact:
Rhonda Boykin
Alameda County Workforce Development Board Director
(510) 259-3842
RBoykin@acgov.org

ATTACHMENTS:

Attachment 1: Appendix: Federal Laws and Policies Related to Data Privacy, Security, and Protecting Personally Identifiable and Sensitive Information

Attachment 2: Staff Confidentiality Agreement

AB 24-02: PII – Attachment 1
APPENDIX:

Federal Laws and Policies Related to Data Privacy, Security, and Protecting Personally Identifiable and Sensitive Information

- **Privacy Act of 1974** (the Privacy Act) – Governs the collection, maintenance, use, and dissemination of PII for individuals maintained in systems of record by Federal agencies. The Privacy Act prohibits the disclosure of information from a system of records without the written consent of the individual unless the disclosure is permissible under one of twelve statutory exceptions. The Privacy Act also provides individuals with a way to seek access to and amendment of their records and establishes various record-keeping requirements. The Privacy Act does not generally apply to PII collected and maintained by subcontractors.

- **Computer Security Act of 1987 –** Passed to improve the security and privacy of sensitive information in Federal computer systems and created a means for establishing minimum acceptable security practices for such systems. It required agencies to identify their computer systems that contained sensitive information, create computer security plans, and provide security training for system users regarding the systems that house sensitive information. It was repealed by the Federal Information Security Management Act (FISMA).

- **FISMA** – Enacted as Title III of the E-Government Act of 2002, required Federal agencies to develop and implement an agency-wide program to safeguard the information and information systems that support the operational assets of the agency, including the assets managed by other agencies, contractors, or subcontractors.

- On May 22, 2006, the Office of Management and Budget (OMB) issued **M-06-15*, Safeguarding Personally Identifiable Information*.** In this memorandum, OMB directed Senior Officials to conduct a review of agency policies and processes and to take necessary corrective action to prevent intentional or negligent misuse of, or unauthorized access to, PII.

- On July 12, 2006, OMB issued **M-06-19*, Reporting Incidents Involving PII and Incorporating the Cost for Security in Agency Information Technology Investments.*** In this memorandum, OMB provided updated guidance for reporting of security incidents involving PII.

- On May 10, 2006, **Executive Order 13402** established the President's Task Force on Identity Theft. The Task Force was charged with developing a comprehensive strategic plan for steps the Federal government can take to combat identity theft and recommending actions which can be taken by the public and private sectors. On April 23, 2007, the Task Force submitted its report to the President, titled "Combating Identity Theft: A Strategic Plan." This report is available at www.idtheft.gov.

- On May 22, 2007, OMB issued **M 07-16, *Safeguarding Against and Responding to the Breach of PII.*** In this memorandum, OMB required agencies to implement a PII breach notification policy within 120 days.

- **NIST SP 800-122, *Guide to Protecting the Confidentiality of PII*** – Released by NIST in April 2010, is a guide to assist Federal agencies in protecting the confidentiality of PII in information systems. The guide explains the importance of protecting the confidentiality of PII in the context of information security and explains its relationship to privacy. The document also suggests safeguards that may offer appropriate levels of protection for PII and provides recommendations for developing response plans for incidents involving PII.

AB 24-02: PII – Attachment 2

STAFF CONFIDENTIALITY AGREEMENT

I, _____ [print name], certify that I have read and understand Action Bulletin (AB) 24-02, Alameda County Workforce Development Board's (ACWDB) Personal Identifiable Information (PII) Protection Policy – and understand that through my work in collaboration with ACWDB may have access to customer's and employer's confidential information. This sensitive information is protected by law, regulation, and policy.

I understand that it is my priority as part of ACWDB's workforce system to protect the confidentiality of all information related individuals and businesses being offered services through the Workforce Innovation and Opportunity Act (WIOA) and any other publicly funded programs.

I understand that the collection, storage, and transmission of sensitive information is protected by federal, state, and local regulations, and violations of stated requirements is punishable and can result in:

- Disciplinary action
- Termination of employment
- Criminal action
- Civil action

By signing this agreement below, I agree to follow and be bound by the terms and conditions regarding the confidentiality of PII.

Signature	Title	Date

ACWDB Staff Use ONLY	
Contractor/Organization/Employer:	
Date Received:	
Received by Staff:	
Other Information:	