Personally Identifiable Information and Confidential Information

Department: Office of Economic & Workforce Development	Effective Date: March 1, 2023
Directive #: WDD 23-46	Supersedes: N/A

PURPOSE

The purpose of this policy is to communicate the requirements for the security of personal and confidential information that the Office of Economic and Workforce Development (OEWD), Workforce Investment San Francisco Board (WISF) and its service providers receive from individuals applying for or receiving services through the Workforce Innovation Opportunity Act (WIOA) or other funding sources.

REFERENCES

- Public Law 113-128-Workforce Innovation and Opportunity Act of 2014
- Privacy Act of 1974
- Social Security Act
- 20 Code of Federal Regulations (CFR) 680.110
- 20 Code of Federal Regulations (CFR) 675.300
- 2 Code of Federal Regulations (CFR) 200.303(e)
- 2 Code of Federal Regulations (CFR) 200.79
- TEGL 39-11 - Guidance on Handling and Protection of Personally Identifiable Information

DEFINITIONS

TEGL 39-11

Personally Identifiable Information (PII) - Office of Management and Budget (OMB) 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 - 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 US Department of Labor 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:

- 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.

- 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.

To illustrate the connection between non-sensitive PII and protected PII, the disclosure of a name, business email 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 program participants is so important.

BACKGROUND

As part of their grant activities, OEWD its service providers will have in their possession Personally Identifiable Information (PII) related to individuals applying for and receiving employment and training services. This information is generally found in participant data sets, performance reports, program evaluations, grant and contract files, and other sources. WIOA requires that Equal Opportunity (EO) data (defined at CFR 675.300) be collected on every individual who applies for WIOA financially assisted aid, benefits, services, or training and who has signified that interest by submitting personal information in their application for services. This confidential information may be shared among the partner agencies of the San Francisco Workforce Delivery system. Agencies awarded federal funds, including WIOA, are required to take aggressive measures to mitigate the risks associated with the collection, storage, and dissemination of sensitive data including PII. (Definitions of PII can be found on page 4 of this document)

POLICY

Federal law, OMB guidance, Department of Labor Employment and Training Administration (DOL ETA), and CA Employment Development Department (EDD) polices require that PII and other sensitive information be protected. OEWD and its service providers must abide by the protocols detailed in this policy to ensure the protection of PII.

Failure to comply with the requirements of this policy, or any improper use or disclosure of PII for an unauthorized purpose, may result in the termination or suspension of grant funds, or the imposition of special conditions or restrictions, or such other actions deemed necessary to protect the privacy of participants or the integrity of data.

The misuse or unauthorized release of personal and confidential information or records by OEWD and its service provider employees and other personnel may be subject to a civil penalty and other applicable sanctions under state and federal law.

PROCEDURE

- PII and sensitive data must not be communicated via email or stored on CD, DVD, thumb drives, etc. unless the device is encrypted.
- 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.
- Social security numbers must not be delivered through email. In the event a staff person receives social security numbers via email, staff must immediately delete the email and subsequently delete the email from the "Deleted Items" folder in Outlook.
- Staff must be discreet when verbally communicating personal and confidential information and ensure the receiver(s) are authorized to receive the information.
- OEWD and its service providers must have policies and procedures that require employees and other personnel, before being granted access to PII, to 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.
- OEWD and its service providers must not extract information from data supplied by the federal awarding agency for any purpose not stated in the grant agreement.
- Access to any PII created by the federal grant must be restricted to only those employees of the grant recipient who need it in their official capacity to perform duties in connection with the scope of work in the grant agreement.
- PII data obtained by OEWD and its service providers through a request from the federal awarding agency must not be disclosed to anyone but the individual requestor except as permitted by the Federal Grant Officer.
- OEWD and its service providers must permit authorized federal, state, and local personnel 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 in this policy. In accordance with this responsibility, OEWD and its service providers must make records applicable to the federally awarded grant available to authorized persons for the purpose of inspection, review, and/or audit.
- OEWD and its service providers must retain data received from the federal awarding agency only for the period of time required to use it for assessment and other purposes, or to satisfy applicable federal records retention requirements. OEWD and its service providers must abide by the Record Retention requirements detailed in OEWD's Record Retention and Public Access Policy.
- Records containing PII must not be left open and unattended (e.g., copies left unattended on desks or print jobs left unattended on the copy machine or printers).
- Personal and confidential information must be stored in a secure location when not in use or shredded if no longer necessary.
- Personal and confidential information must not be tossed in the regular trash or recycle bins. Use appropriate methods for destroying sensitive PII in paper files, (i.e., shredding or using a burn bag) and securely deleting sensitive electronic PII.

- Archive boxes must be clearly marked as containing personal and confidential information.

Medical and Disability Information
Whether written or oral and regardless of format, staff must maintain confidentiality of the following:

- 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 kept in a separate locked file (if in paper form) and apart from working files.
- 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 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.

When all services, including follow-up services, are complete and the participant file is ready to be archived, participant medical and disability-related information that had been previously filed away from the active file must be placed in a sealed envelope and marked "Medical and Disability Information" and secured in the participant file.

Authorization to Share Confidential Information and Records
In accordance with federal and state law, individuals applying for WIOA, or other federally funded services must be provided an opportunity to submit written authorization allowing the service provider to share their personal and confidential information and records. Each individual must also be informed that they can request their personal and confidential information not be shared among the partner agencies of the San Francisco Workforce Delivery system and this request does not affect their eligibility for services. OEWD utilizes the Release of Information form for this purpose.

Individuals seeking services from OEWD and its service providers must be informed, in writing via the Release of Information form, that their personal and confidential information:

- May be shared among the OEWD partner staff and sub-contractors
- Is used only for the purpose of delivering services and that further disclosure of their confidential information is prohibited, and
- Will not be shared among the partners of the San Francisco Workforce Delivery system if the individual declines to share their confidential information and the decline to share will not impact their eligibility for services

Individuals applying for services must sign and date the Release of Information form attesting they have read and understand how their information will be shared and protected.

INQUIRIES

Inquiries should be addressed to the OEWD Director of Workforce Strategy at (415) 701-4848 or email workforce.connection@sfgov.org.

OEWD and its service providers shall follow this policy. This policy will remain in effect from the date of issue until such time that a revision is required.