WORKFORCE DEVELOPMENT
BOARD OF MADERA COUNTY

USE AND CONFIDENTIALITY OF PARTICIPANT PERSONALLY IDENTIFIABLE INFORMATION (PII)

EDD Revision Date: N/A
WDB Review Date: 10/17/19

EXECUTIVE SUMMARY

PURPOSE:

This document establishes the Workforce Development Board of Madera County's policy on the use and confidentiality of Participant Personally Identifiable Information (PII)

REFERENCES:

Law

- Workforce Innovation and Opportunity Act of 2014 (WIOA)
- Privacy Act of 1974, Section 7
- California SB168, Title 1.81.1 – Confidentiality of Social Security Numbers
- California AB763 – Privacy: Social Security Numbers
- Federal Information Security Management Act (FISMA)

Federal Guidance

- Training and Employment Guidance Letter (TEGL) 05-08 – Policy for collection and Use of Workforce System Participants' Social Security Numbers
- TEGL 39-11 – Guidance on the Handling and Protection of Personally Identifiable Information (PII)
- OMB Memorandum M-07-16 – Safeguarding Against and Responding to the Breach of Personally Identifiable Information
- NIST SP 800-122 – Guide to Protecting the Confidentiality of PII

ATTACHMENTS:

- Attachment A: Staff/Representative Confidentiality Agreement
- Attachment B: Participant Confidentiality Rights
- Attachment C: Definitions of Key Terms

POLICY:

Employees, contractors, consultants, and volunteers of the WDB (herein "staff and representatives") may be exposed to participant information that is confidential and/or

privileged and proprietary in nature. As part of grant activities, staff and representatives may have access to large quantities of personally identifiable information (PII) relating to individual program participants. This information could be found in participant files and data sets, performance reports, program evaluations, grant and contract files, and other sources.

The WDB expects all staff and representatives to respect the privacy of clients and to maintain their personal and financial information as confidential. Access to any PII must be restricted to only those staff and representatives who need it in their official capacity to perform duties pertaining to the scope of work in the grant or contract agreement. No information may be released without appropriate authorization.

Customer Awareness

Individuals must be informed in writing how their information will be used and that their information will be protected and that their personal and confidential information:

- May be shared among federal and state agencies, partner staff and contractors;
- Is used only for delivering services and that further disclosure of their confidential information is prohibited; and that
- PII will be used for grant and eligibility purposes only.

Every individual receiving WIOA or other WDB services must read, sign and date a Release of Information to share their information with partner agencies. Individuals must be informed that they can request that their information not be shared among partner agencies and that this does not affect their eligibility for services.

Staff and representatives should engage in practical ways to reduce potential security breaches and protect sensitive information and PII by:

- Reducing the volume of collected and retained information to the minimum necessary;
- Limiting access to only those individuals who must have such access; and
- Using encryption, strong authentication procedures, and other security controls to make information unusable by unauthorized individuals.

Protecting Information

PII and confidentiality require special precautions to protect them from unauthorized use, access, disclosure, modification, and destruction. Confidentiality means that data, reports, and other outputs are safeguarded against unauthorized access. Staff will exercise extreme care and caution when working with confidential information to ensure the privacy of the applicant or customer.

Physical Data Protection Requirements

All sensitive or PII data obtained should be stored in an area that is always physically safe from access by unauthorized persons. Staff and representatives must not leave personal and confidential information left open and unattended.

When a staff or representative's desk is unattended, it is the staff or representative's

responsibility to ensure that personal and confidential information, including PII, is secured in closed containers such as locked drawers or offices when not in use. This means that all documents containing personal and confidential information must not be left on desks, fax machines, printers, or photocopiers unattended. Desktops and computers will be kept clear of papers and/or files containing confidential information that are not being used. Desktops and computers will be kept clear of confidential information during non-business hours.

Any papers containing PII and/or confidential information are to remain in the office. All discarded paper containing confidential information shall be placed in a locked shredder bin or shredded.

Any participant files stored for performance or archiving purposes must be clearly marked as containing personal and confidential information. Staff and representatives should retain participant PII only for the period required for assessment or performance purposes. Thereafter, all data must be destroyed by a qualified company to minimize risk of breach.

Electronic Data Protection Requirements

To safeguard WDB's electronically stored data, each user will receive a designated and authorized log-on(s) and password(s) that restrict users to the applications or functions commensurate with their assigned responsibilities, supporting an appropriate segregation of duties. This is such that unauthorized persons cannot reasonably retrieve the information by means of a computer.

The WDB expects all staff to secure mobile equipment, such as laptop computers and other devices that may have PII stored on them. Devices should be password protected and safeguarded when not in use. Accessing and storing data containing PII on personally owned equipment at off-site locations, such as the employee's home, and on non-managed IT services, such as Google or Yahoo, is prohibited.

Transmission of Confidential Information

Staff and representatives should avoid communicating sensitive information or PII about an applicant or participant to partner agencies or other staff via email. If it is necessary, staff and representatives must ensure that the intended recipient is the only individual that has access to the information and that the recipient understands they must also protect the information. Staff and representatives must only communicate sensitive information or PII through WDB emails and not through third party or personal email addresses.

PII and other sensitive data transmitted via email or stored on mobile data storage (such as thumb drives) must be encrypted. Staff and representatives must not e-mail unencrypted sensitive PII to any entity, including the Department of Labor, WDB staff, or contractors. Staff and representatives should discourage participants from emailing personal and confidential information to their case managers.

Any information posted to social media sites is considered public record and is subject to public disclosure. No sensitive information or PII should be posted to social media sites.

Care shall also be taken to ensure that unauthorized individuals do not overhear any discussion of confidential information.

Social Security Numbers

Social security numbers are protected as high-risk information. When requesting a participant's social security number, staff and representatives should explain how the social security number will be used and how the participant's privacy will be ensured.

Staff must request a participant's social security number when offering the following services:

- Staff-assisted service related to eligibility determination, job search activity, and employment;
- All training and educational services; and
- Self-services through CalJOBS.

However, an individual is not required to provide their social security number to receive WIOA services, and services cannot be denied to an individual due to their refusal to disclose their social security number.

Whenever possible, staff and representatives should use unique identifiers for participant tracking instead of social security numbers. While social security numbers may be needed for initial eligibility or performance purposes, a unique identifier should be linked to each individual record and used thereafter. This includes such records as training or contract documents. If social security numbers are to be used for specific tracking purposes, they must be stored or used in such a way that it is not attributable to the individual. For example, a training document should not include the participant name and social security number, rather the participant name and a truncated social security number.

Social Security numbers may not be listed on anything mailed to a client or to another agency unless required by law, or the document is a form or application. Social Security numbers may not be left on a voice mail message.

Medical and Disability Records

Medical and disability records are additionally protected as confidential information. To ensure the information is protected, any medical or disability records must be kept separately from working participant files and kept in a secured physical and/or electronic location. Only the portion of the participant's information that reveals the presence of a disability or other data elements should be included in the participant's file to minimize staff and representative access to medical files.

Once collected, access to the medical file should be limited and only accessed:

- With the approval of program management and only when necessary for WIOA service delivery;
- By first aid and safety personnel in the event of an emergency; or

- By local, state, or federal monitors.

Participant medical and confidential information will remain in the secured location until file is shredded.

Security Breaches

Any staff or representative who becomes aware of any actual or attempted PII security breach resulting from the inadvertent or intentional leak of release of confidential information, including PII, shall immediately inform their direct supervisor. PII security incidents include, but are not limited to, any event (intentional or unintentional) that causes the loss, damage, or destruction, or unauthorized access, use, modification, or disclosure of information assets. The system or device affected by a PII security incident shall be immediately removed from operation. It shall remain removed from operation until correction and mitigation measures are applied.

Supervisors should assess the likely risk of harm caused by the breach and then assess the level of breach. Supervisors should bear in mind that notification when there is little or no risk of harm might create unnecessary concern and confusion.

Four factors should be considered to assess the likely risk of harm:

- Nature of the Data Elements Breached
- Number of Individuals Affected
- Likelihood the Information is Accessible and Usable
- Likelihood the Breach May Lead to Harm

WDB will inform the California Employment Development Department of breaches believed to cause harm. Breaches subject to notification requirements include both electronic systems as well as paper documents.

Individuals assessing the likely risk of harm due to a security breach should exercise the objectivity principle, which requires individuals to show the highest professional objectivity level in collecting, assessing, and communicating information about the breach examined. Further, assessors are expected to perform a balanced assessment of every relevant situation and they must not be influenced by their own or other people's interest while forming judgments.

Staff Compliance

All employees must sign an acknowledgement that they have read the policy, understand the confidential nature of participant data and the potential sanctions for improper disclosure, and agree to abide by all other requirements and terms contained therein.

Unauthorized disclosure of confidential or privileged information is a serious violation of this policy. Any failure to comply with confidentiality requirements identified in this policy may result in termination or suspension of contract or employment, or the imposition of special conditions or restrictions to protect the privacy of participants or the integrity of PII data. Misuse or noncompliance with PII data safeguards could lead to civil and criminal

sanctions per federal and state laws.

Staff and representatives are expected to return materials containing privileged or confidential information at the time of separation from employment or expiration of service.

Disclaimer
This policy is based on WDB's interpretation of the statute, along with the Workforce Innovation and Opportunity Act; Final Rule released by the U.S. Department of Labor, and federal and state policies relating to WIOA implementation. This policy will be reviewed and updated based on any additional federal or state guidance.

INQUIRIES:

If you have questions, please contact the Executive Director or designee at (559) 662-4500.

Definitions of Key Terms

Personally Identifiable Information (PII) as defined by OMB Memorandum M-07-16 is any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal information that is linked or linkable to a specific individual.

There are two types of PII as defined by the U.S. Department of Labor in TEGL 39- 11 that are based on the "risk of harm" that could result from the release of the PII:

- Protected PII – is any information that if disclosed could result in harm to the individual whose name or identify is linked to that information. Examples include, but are not limited to, social security numbers, credit card numbers, bank account numbers, personal telephone numbers, ages, birthdates, marital status, spouse names, educational history, biometrics identifiers, medical history, financial information, and computer passwords.
- Non-Sensitive PII – is information that if disclosed, by itself, could not reasonably be expected to result in personal harm as it is not linked or closely associated with any protected or unprotected PII. Examples include first and last names, e-mail addresses, business addresses, business telephone numbers, general education credentials, gender, or race.

A combination of non-sensitive PII could potentially be categorized as protected PII. As example, a name and business e-mail address will not result in a high degree of harm to an individual. A name linked to a social security number and date of birth could result in identity theft.

A **Security Breach** as defined by TEGL 39-11 is used to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.

Sensitive Information as defined by TEGL 39-11 is any unclassified information whose loss, misuse or unauthorized access to or modification of could adversely affect the interest of the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act.