WORKFORCE INVESTMENT BOARD OF TULARE COUNTY **WORKFORCE INNOVATION AND OPPORTUNITY ACT TITLE I**	**DATE: June 12, 2019** **SUBJECT:** **USE AND CONFIDENTIALITY OF PARTICIPANT'S PERSONALLY IDENTIFIABLE INFORMATION (PII)**

WIB DIRECTIVE **TUL 19-03**

APPROVED BY
WORKFORCE INVESTMENT BOARD
MINUTES OF 06-12-2019

TO: WIB Subrecipients
WIB Staff

SUBJECT: USE AND CONFIDENTIALITY OF PARTICIPANT'S PERSONALLY IDENTIFIABLE INFORMATION (PII)

EXECUTIVE SUMMARY

It is the policy of the Workforce Investment Board of Tulare County (WIB) to protect the privacy of all applicants for program services, as well as the privacy of all customers and clients receiving program services. The purpose of this policy is to describe how the WIB will protect all personally identifiable information (PII) on applicants and customers, and the consequences for not adhering to these safeguards.

Under the Workforce Innovation and Opportunity Act (WIOA), staff obtains personal and confidential information from individuals as part of eligibility determination and continuation of services. WIOA and other federal and state regulations governing information sharing stipulate implementation of confidentiality policies and procedures.

Personal information will be treated in the strictest confidence and will not be shared outside of the WIB without written authorization, except for auditing purposes and other grantor-imposed information-sharing requirements. The purpose of this policy is to specify the requirements for the use, storage, and security of sensitive and confidential information.

REFERENCES

- 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)

- 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
- County of Tulare – Information Technology Security Program, June 20, 2017
- County of Tulare – Administrative Regulation No. 36

POLICY AND PROCEDURES

WIB staff and WIB subrecipients may be exposed to participant information which is confidential and/or privileged and proprietary in nature. As part of grant activities, staff 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 WIB expects all staff 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 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 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 WIB 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 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 physically safe from access by unauthorized persons at all times. Staff must not leave personal and confidential information left open and unattended.

When a staff's desk is unattended, it is the staff'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 subrecipients offices, except invoices, contracts and on occasion other paperwork may be transported to other locations for a specific purpose. 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 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 WIB's electronically stored data (CalJOBS), 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 WIB 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 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 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 must only communicate sensitive information or PII through WIB or subrecipients 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 must not e-mail unencrypted sensitive PII to any entity, including the Department of Labor, EDD, WIB staff, or WIB subrecipients. Staff 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 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;
- 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 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 electronic 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 element 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.

When all WIOA or other WIB services are complete and the participant file is ready to be archived, participant medical and disability-related information must be placed in a sealed envelope and marked "Medical and Disability Information."

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. The direct supervisor will inform the WIB staff of the breach. 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.

WIB staff should assess the likely risk of harm caused by the breach and then assess the level of breach. WIB staff 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

WIB will inform the California Employment Development Department of any CalJOBS 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 staff with access to participant PII and/or confidential information must sign an acknowledgment 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 is 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 WIB'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.

ACTION

Please bring this directive to the attention of all WIB Subrecipients and WIB Staff.

INQUIRIES

Please direct inquiries about this directive to the WIB at (559) 713-5200.

Adam Peck
Executive Director

AP:CE:llg

Attachment A – Staff Confidentiality Agreement

Attachment A

STAFF CONFIDENTIALITY AGREEMENT

I, _____ [print name] certify that I have read and understand the Workforce Investment Board of Tulare County's (WIB) policy on **USE AND CONFIDENTIALITY OF PARTICIPANTS' PERSONALLY IDENTIFIABLE INFORMATION (PII)**. I understand that I may have access to customer and employer confidential records as part of my employment, contracting, or volunteer work with the WIB. Confidential information provided to our agency by any participant or by any federal, state, or county entity is protected by law, regulation, and policy.

I understand that it is my responsibility as part of the workforce development system in Tulare County to protect the confidentiality of all Workforce Innovation and Opportunity Act (WIOA) applicants and participants, as well as customers utilizing the Tulare County Employment Connection, an affiliate of the America's Job Centers of California (AJCC) system. I understand that in the workforce system's collection, usage, storage and transmission of customer information, the tenets of confidentiality are to be strictly enforced.

I understand that I have the responsibility to know whether information is protected. If I have any questions regarding whether particular information is confidential, I understand it is my responsibility to check with my supervisor.

I understand that unauthorized access, use, modification, or disclosure of confidential information is a crime under state and federal laws, including but not limited to California Information Privacy Act §1798.53-§1798.57, CA Penal Code §502, §2111 of the Unemployment Insurance Code, and §10850 of the Welfare and Institutions Code. I understand that violation of this policy could result in:

- Disciplinary action
- Criminal action (including incarceration
- Termination of employment
- Civil action

By signing below, I agree to follow and be bound by the terms and conditions regarding confidentiality of personal information contained therein. WIB staff or their designee have answered any questions I may have had regarding this policy.

Signature:_____

Name:_____ Date: _____