Fresno Regional Workforce Development Board

A proud member of America's Job Center of California℠ Network

2125 Kern Street, Suite 208 • Fresno, California 93721 • 559.490.7100 • Fax 559.490.7199 • www.frwdb.net

Blake Konczal, Executive Director

OPERATIONAL DIRECTIVE

FRWDB OD # 07-23 **Date Released: June 30, 2023**

To: All Fresno Regional Workforce Development Board Providers of Services

From: Blake Konczal, Executive Director

Effective Date: July 3, 2023

Subject: FRWDB Confidential Information

Applicable Program: All

Revision History: Initial Release

The purpose of the OD is to communicate the requirement that all Provider of Services staff formally acknowledge they are handling confidential information while performing their job duties and they are aware of the ramifications of not being in compliance with handling Personally Identifiable Information (PII) procedures.

The Operational Directive (OD) supersedes OD 32-02, Confidential Information.

The OD references OD 08-23, Information Systems Security Process and OD 06-23, Designation of Information Security Staff.

The protection of confidential information requires special precautions that include a Confidentiality Statement being signed by all Providers of Services staff. The statement restricts the unauthorized use, access, disclosure, modification, and destruction of confidential information. Providers of Services and Partners will exchange various kinds of personal information which may include but is not limited to participant and employer data, applications, program files and data bases. All data and information are to be considered confidential.

Definitions

Personally Identifiable Information (PII): PII means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. There are two levels of PII:

a. Protected PII: Information that, if disclosed, could result in harm to the individual whose name or identity is linked to that information. Examples of Protected PII are:
   i. Social Security Numbers (SSN)
   ii. Credit card numbers
   iii. Bank account numbers
   iv. Home telephone numbers
   v. Ages

vi. Birthdays,
vii. Marital status
viii. Spouse names
ix. Educational history,
x. Biometric identifiers (fingerprints, voice prints, retinal scans, etc)
xi. Medial history
xii. Financial information
xiii. Computer passwords

b. Non-sensitive PII: Information that, if disclosed, could not reasonably be expected to result in personal harm. It is information that is not linked or closely associated with any protected or non-protected PII. However, depending on the circumstances, a combination of these items could potentially be categorized as protected PII. Examples of Non-Protected PII:

i. First and last names
ii. Physical addresses (in most cases)
iii. E-mail addresses
iv. Business addresses
v. Business telephone numbers
vi. General education credentials
vii. Gender
viii. Race

c. Verbal PII: Conversations include, but are not limited to:

i. Discussions in open areas (i.e.: hallways, breakrooms)
ii. Telephone conversations
iii. Speakerphones
iv. Video calls/conferencing

Requirements

All Providers of Services must:

a. Keep in the strictest of confidence all information that is exchanged between them and other authorized agencies or employers, and make such information available to only authorized employees on a "need to know" basis.

b. Not disclose any confidential information to a third party, unless a signed and current release of confidential information has been received that includes:

i. written instructions,
ii. identification of all parties
iii. Describes the confidential nature of the information to be released
iv. Notice of potential penalties for unauthorized use or disclosure

c. When applicable, store and process information in electronic format in such a way that unauthorized persons can not reasonable retrieve the information by means of a computer remote terminal or other method.

d. Promptly return to the other party confidential information when its use ends or destroy the confidential information utilizing an approved method of destruction (i.e.: shredding, or certified/witnessed destruction, deleted from a database).

e. When entering into a third-party agreement when services are to be provided, the agreement must include an assurance that each party will act in accordance with the requirements of the OD and applicable law. In no even shall information be disclosed to any individual outside of that third party's authorized staff, without expressed written authorization.

f. Designate an employee who shall be responsible for overall security and confidentiality of its data and information systems (see OD 06-23, Designated Information Security Officer).

g. Have a dated and signed Staff Confidentiality Acknowledgement (From# QUA-100) in each staff person's personnel file, regardless of job title or job description.

    i. The employee must be provided a copy of the signed and dated statement.

Please contact the FRWDB Information & General Services manager if any questions.

Form:

QUA-100, Staff Confidentiality Acknowledgement Form