Fresno Regional Workforce Development Board

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

2125 Kern Street, Suite 208 • Fresno, California 93721 • 559.490-7100 • Fax 559.490.7199 •
www.workforce-connection.com

Blake Konczal, Executive Director

POLICY BULLETIN

FRWDB PB # 01-18 **Date Released: June 13, 2018**

To: All Fresno Regional Workforce Development Board Providers of Services

From: Blake Konczal, Executive Director

Effective Date: June 13, 2018

Subject: Handling and Protection of Personally Identifiable Information Policy

Applicable Program: All

Revision History: Initial Release

This Policy Bulletin (PB) references ETA TEGL 39-11, Handling and Protection of Personally Identifiable Information (PII), OMB Guidance 2 CFR 200 §200.79, Operational Directive (OD) 10-12, Record Retention and Storage; OD 6-18, Casefile Security.

Federal agencies are required to take aggressive measures to mitigate the risks associated with the collection, storage, and dissemination of sensitive data, including Personally Identifiable Information (PII) that is not otherwise publicly available. This includes sub-recipients and direct grantees of federal agencies.

As such, the Fresno Regional Workforce Development Board (FRWDB) staff has developed this policy that communicates the requirements and responsibilities to its sub-recipients pertaining to the acquisition, handling and transmission of PII.

Definitions

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:

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 - 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: Information that, if disclosed by itself, 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-Sensitive PII: first and last names, physical address (in most cases), e-mail addresses, business addresses, business telephone numbers, general education credentials, gender, or race.

Handling of PII

Protected PII and other sensitive information are required to be protected. Protected PII and Non-sensitive PII can be found in multiple formats, including but not limited to:

- Hardcopy (paper, files, original documents, printed documents, copies);
- Electronic information (email, electronic or computer-based files, electronic images, multi-media files (voicemails, video, photographs); or
- Verbal – when discussing an individual's PII in a non-private setting.

Each format introduces unique challenges and circumstances to insure that Protected PII is not transmitted to unauthorized persons.

Hardcopy Protected PII

- Must be placed in an area that is physically safe from access by unauthorized persons at all times.
- Protected PII is not to be left unattended.
    - Must be stored in locked cabinets or areas when not in use.
- When utilizing a photocopier to scan or copy documents containing Protected PII, the equipment and documents are never to be left unattended.
    - Secure printing (ability to "print to hold" and/or "password protected") shall be used whenever possible.
    - Where secure printing is not available, documents with Protected PII shall not be printed in an unsecure area.
- Clients and visitors must be accompanied by authorized staff at all times anywhere in non-public areas of the facility.
- Clients and visitors are not to be left alone in offices or cubicles where Protected PII is unsecure.
- Disposing of Protected PII documents.
- Shall be either shredded in a mechanical shredder or deposited into identified locked disposal receptacles.
- Archived Documents - All providers of services are required to insure all archived files are maintained in locked storage and disposed of in accordance with FRWDB OD 10-12, Record Retention and Storage.

Electronic Protected PII

- Protected PII is not to be transmitted via email or stored on CDs, thumb drives, or other mobile storage devices.

- When electronic Protected PII must be transmitted between authorized personnel, a secure method must be used. Examples of secure file sharing methods are:
    - Secure File Transfer Protocol (SFTP),
    - FRWDB's Egnyte file sharing application,
    - Utilization of organization's shared network folders.
- Computers are to be locked when unattended,
    - Either user logged off or the computer access locked.
- All computer servers containing databases with Protected PII and network firewalls (software/hardware) must be in a physically secured location only accessible by authorized Technical and Facilities personnel.
- All Protected PII data collection interfaces and reporting tools, accessible via the Internet must have secure, encrypted protocols in place.
- Accessing, processing, and storing of Protected PII data on personally owned equipment, at off-site locations e.g., employee's home, personal email, Cloud services (such as iCloud) is strictly prohibited.

Verbal PII

Conversations that include Protected PII or Non-sensitive PII should be done in a discrete manner so as not to disseminate any PII unintentionally to unauthorized persons.

Conversations include, but not limited to, discussions in open areas (i.e. breakrooms, hallways), telephone calls using speaker phone, video conferencing (Skype or webinars).

In Case of Breach

Definition: A breach is when it is known or suspected, that Protected PII has been released as a result of any of the following incidents:

- Theft of hardcopy documents that contain Protected PII,
- Missing computer known to contain Protected PII,
- Missing storage device known to contain Protected PII,
- Evidence of non-authorized access of database(s) that contains Protected PII.

FRWDB staff will develop and implement Operational Directive(s) and internal FAWIC procedures that will provide specific direction to sub-recipients and FRWDB staff concerning what to do if a Breach of Protected PII is suspected. These documents will include:

- Who to notify at the FRWDB
- A Damage Assessment process
- Action Plan for:
    - notification:
        - Affected staff, partners, and/or participants,
        - State (if required),
        - Chief Local Elected Officials (if required).
    - To contain further loss,
    - To recover Protected PII, if possible.