

January 9, 2018

DYLAN WRIGHT
DIRECTOR
OC COMMUNITY RESOURCES

CYMANTHA ATKINSON
DEPUTY DIRECTOR
OC COMMUNITY RESOURCES

JENNIFER HAWKINS, DVM
DIRECTOR
OC ANIMAL CARE


RENEE RAMIREZ
DIRECTOR
OC COMMUNITY SERVICES

JULIA BIDWELL
DIRECTOR
HOUSING COMMUNITY
DEVELOPMENT & HOMELESS
PREVENTION

STACY BLACKWOOD
DIRECTOR
OC PARKS

HELEN FRIED
COUNTY LIBRARIAN
OC PUBLIC LIBRARIES

To: WIOA Subrecipients of the Orange County
Development Area

From: Brian Rayburn 
Interim Director

Subject: **Personally Identifiable Information
Information Notice No. 17-OCDB-07
Supersedes Information Notice 02-OCWDA-60**

PURPOSE:

This policy provides guidance to subrecipients on compliance with the requirements of handling and protecting Personally Identifiable Information (PII).

This policy supersedes Information Notice 02-OCWDA-60 dated June 17, 2003.

EFFECTIVE DATE:

This notice is effective on the date of issuance.

REFERENCES:

- Training and Employment Guidance Letter (TEGL) No. 39-11

BACKGROUND:

Subrecipients may have in their possession large quantities of PII relating to their organization and staff; partner organizations and their staff; and individual program participants. This information is generally found in personnel files, participant data sets, performance reports, program evaluations, program and contract files and other sources. Subrecipients are required to take aggressive measures to mitigate the risks associated with the collection, storage, and dissemination of sensitive data including PII.

POLICY AND PROCEDURES:

Definitions

- 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.



**ORANGE COUNTY
DEVELOPMENT BOARD
1300 SOUTH GRAND
BLDG. B, THIRD FLOOR
SANTA ANA, CA 92705
PHONE: 714.480.6500
FAX: 714.834.7132**



- Protected PII and non-sensitive PII – the Department of Labor (DOL) 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.
 1. *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.
 2. *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 e-mail 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.

Requirements

Federal law, OMB Guidance, State and local polices require that PII and other sensitive information be protected. The Orange County Development Board (OCDB) has examined the ways its subrecipients handle PII and sensitive information and has determined that to ensure OCDB compliance with Federal law and regulations, subrecipients must secure transmission of PII and sensitive data developed, obtained, or otherwise associated with OCDB funded programs.

In addition to the requirement above, all subrecipients must also comply with all of the following:

- To ensure that such PII is not transmitted to unauthorized users, all PII and other sensitive data transmitted via e-mail or stored on CDs, DVDs, thumb drives, etc., must be encrypted using a Federal Information Processing Standards (FIPS) 140-2 compliant and National Institute of Standards and Technology (NIST) validated

cryptographic module¹. Subrecipients must not e-mail unencrypted sensitive PII to any entity.

- Subrecipients must take the steps necessary to ensure the privacy of all PII obtained from participants and/or other individuals and to protect such information from unauthorized disclosure. Subrecipients must maintain such PII in accordance with the Federal standards for information security described in this policy and any updates to such standards provided by the OCDB.
- Subrecipients shall ensure that any PII used has been obtained in conformity with applicable Federal and state laws governing the confidentiality of information.
- Subrecipients further acknowledge that all PII data obtained be stored in an area that is physically safe from access by unauthorized persons at all times and the data will be processed using issued equipment, managed information technology (IT) services, and designated locations approved by OCDB. Accessing, processing, and storing of PII data on personally owned equipment, at off-site locations e.g., employee's home, and non-subrecipient managed IT services, e.g., Yahoo mail, is strictly prohibited unless approved by the OCDB.
- Subrecipient employees and other personnel who will have access to sensitive/confidential/proprietary/private data must be advised of the confidential nature of the information, the safeguards required to protect the information, and that there are civil and criminal sanctions for noncompliance with such safeguards that are contained in Federal and state laws.
- Subrecipients must have their policies and procedures in place under which subrecipient employees and other personnel, before being granted access to PII, 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.
- Subrecipients must not extract information from data supplied by the OCDB for any purpose not stated in their agreement.
- Access to any PII created must be restricted to only those employees of the subrecipient who need it in their official capacity to perform duties in connection with the scope of work in the agreement.
- All PII data must be processed in a manner that will protect the confidentiality of the records/documents and is designed to prevent unauthorized persons from retrieving such records by computer, remote terminal or any other means. Data

¹ For more information on FIPS 140-2 standards and cryptographic modules, subrecipients should refer to FIPS PUB 140-2, located online at: <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>.

may be downloaded to, or maintained on, mobile or portable devices only if the data are encrypted using NIST validated software products based on FIPS 140-2 encryption. In addition, wage data may only be accessed from secure locations.

- PII data obtained by the subrecipient through a request from OCDB must not be disclosed to anyone but the individual requestor except as permitted by the OCDB.
- Subrecipients must permit OCDB to make onsite inspections during regular business hours for the purpose of conducting audits and/or conducting other investigations to assure that the subrecipient is complying with the confidentiality requirements described above. In accordance with this responsibility, subrecipients must make records applicable to their agreement available to authorized persons for the purpose of inspection, review, and/or audit.
- Subrecipients must retain data received from OCDB only for the period of time required to use it for assessment and other purposes, or to satisfy applicable records retention requirements, if any. Thereafter, the subrecipient agrees that all data will be destroyed, including the degaussing of magnetic tape files and deletion of electronic data.

A subrecipient's failure to comply with the requirements identified in this policy, or any improper use or disclosure of PII for an unauthorized purpose, may result in the termination or suspension of the agreement, or the imposition of special conditions or restrictions, or such other actions as the OCDB may deem necessary to protect the privacy of participants or the integrity of data.

Recommendations

Protected PII is the most sensitive information that may be encountered and it is important that it stays protected. Subrecipients are required to protect PII when transmitting information, but are also required to protect PII and sensitive information when collecting, storing and/or disposing of information as well. Outlined below are some recommendations to help protect PII:

- Before collecting PII or sensitive information from participants, have participants sign releases acknowledging the use of PII for program purposes only.
- Whenever possible, OCDB recommends the use of unique identifiers for participant tracking instead of SSNs. While SSNs may initially be required for performance tracking purposes, a unique identifier could be linked to the each individual record. Once the SSN is entered for performance tracking, the unique identifier would be used in place of the SSN for tracking purposes. If SSNs are to be used for tracking purposes, they must be stored or displayed in a way that is not attributable to a particular individual, such as using a truncated SSN.

- Use appropriate methods for destroying sensitive PII in paper files (i.e., shredding or using a burn bag) and securely deleting sensitive electronic PII.
- Do not leave records containing PII open and unattended.
- Store documents containing PII in locked cabinets when not in use.
- Immediately report any breach or suspected breach of PII to the OCDB.

ACTION:

Bring this policy and procedure to the attention of all staff.

INQUIRIES:

If you have any questions regarding this policy, please contact your Contract Administrator at 714-480-6500.

