



DATE: January 4, 2020
DIRECTIVE NO: 58-20
RECISSION: La Cooperativa Directive No. 46-19
TO: All La Cooperativa and Subrecipient Personnel
SUBJECT: Personally Identifiable Information and Other Confidential Information

PURPOSE:

The purpose of this directive is to provide guidance to La Cooperativa and subrecipient personnel on the requirements for handling PII and other confidential information and to include a revision to the Release of Information Requirements.

For future oversight reviews please ensure that PII information is redacted from the submission of documentation related to participants or staff.

REFERENCES:

- 2 CFR Chapter 200.337 - Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards
- Training and Employment Guidance Letter (TEGL) No. 39-11 - issued June 28, 2012

DEFINITIONS:

Personally Identifiable Information (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 that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, public Web sites, and university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.

1107 – 9th St., Ste 420, Sacramento, CA 95814 - (916) 388-2220 - Fax (916) 388-2425

Teresa Hitchcock
Chairperson



Marco Lizarraga
Executive Director

Subaward means an award provided by a pass-through entity to a subrecipient for the subrecipient to carry out part of a Federal award received by the pass-through entity. It does not include payments to a contractor or payments to an individual that is a beneficiary of a Federal program. A subaward may be provided through any form of legal agreement, including an agreement that the pass-through entity considers a contract.

Subrecipient means a non-Federal entity that receives a subaward from a pass-through entity to carry out part of a Federal program; but does not include an individual that is a beneficiary of such program. A subrecipient may also be a recipient of other Federal awards directly from a Federal awarding agency.

POLICY AND PROCEDURES:

There are 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 – information that, if disclosed, could result in harm to the individual whose name or identity is linked to the 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, biometric identifiers (fingerprints, iris scans, etc.), medical history, financial information and computer passwords.
2. Non-sensitive PII – 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 include 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.

Federal Requirements

The U. S. Department of Labor, Employment and Training Administration (ETA) has established the following requirements for the handling of PII.

1. All PII and other sensitive data transmitted via email or stored 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 module. Unencrypted sensitive PII cannot be emailed.

2. Data must be processed in a manner to protect the confidentiality of the records/documents and is designed to prevent unauthorized persons from retrieving such records.
3. La Cooperativa staff and its subrecipients must ensure privacy of all PII obtained from participants and/or other individuals and protect such information from unauthorized disclosure.
4. PII data must be stored in an area physically safe from access by unauthorized persons at all times. Accessing, processing and storing of subgrant PII data on personally owned equipment at off-site locations is prohibited.
5. La Cooperativa staff and its subrecipients who will have access to PII must be advised of the confidential nature of the information, the safeguards to protect the information and the civil and criminal sanctions for noncompliance with such safeguards. Personnel must acknowledge their understanding of these compliance requirements and their liability for improper disclosure.
6. Data may not be obtained or used for any purpose other than those required by the programs. Access to data is restricted to only those individuals who need it in their official capacity to perform duties in connection with the scope of work.

Release of Information Requirements

1. **All personally identifiable information and other confidential information shall be redacted from requests for participant or staff documentation made by the Employment Development Department and the U. S. Department of Labor.**
2. Prior to releasing a WIOA participant's information, an authorization form must be signed by the individual.
3. Requests for information from local law-enforcement agencies should be accommodated without compromising participant confidentiality. Requests for participant files, documents or other printed personal information to other than representatives of La Cooperativa, the Employment Development Department or ETA shall not be released without a subpoena.
4. The Executive Director of La Cooperativa should be informed of requests for information made by law enforcement, as well as requests for information made by subpoena. If in doubt about a situation, the Executive

Director of La Cooperativa should be contacted.

5. The various screens at subrecipient locations containing confidential information are to be used only by assigned staff and only for authorized purposes. The available screens are not to be printed, duplicated or disseminated in any unauthorized manner. This includes job seeker/participant data, business data and unemployment information.

Recommendations

Use appropriate methods for destroying sensitive PII in paper files, such as shredding, and securely deleting sensitive electronic PII.

Social Security Number Confidentiality Requirements

All La Cooperativa staff and subrecipient personnel have a responsibility to keep Social Security numbers of job seekers and other individuals in your possession secure.

The disclosure of Social Security numbers to unauthorized persons or entities is prohibited. La Cooperativa staff and subrecipient personnel will not knowingly display, disclose, transfer, or unlawfully use the Social Security number of any employee, participant, or other individual in any manner that violates the Social Security Protection Act of 2004 or the Privacy Act of 1974.

Social Security numbers should only be collected where required by federal or state law. If a unique personal identifier is needed, a substitute for the Social Security number shall be used in its place.

Documents, materials, or computer screens displaying Social Security numbers shall be kept out of public view at all times.

Documents containing Social Security numbers shall only be sent where permitted by state and federal law. A Social Security number may be included in a mailed document where:

1. It is sent as part of an application or enrollment process initiated by the individual.
2. It is sent to establish, confirm the status of, service, amend or terminate an account, contract, employee or health insurance benefit – or to confirm the accuracy of a Social Security number of an individual who has an account, contract, policy, or employee or health insurance benefit.
3. It is sent for the purpose of compliance with proper administration of the federal/state Unemployment Insurance program.

4. It is contained in a public record and is mailed in compliance with the Freedom of Information Act. Otherwise, the Social Security number shall be redacted.
5. It is mailed by, or at the request of, an individual whose Social Security number appears in the document or information of his or her parent or legal guardian.
6. The number shall not be revealed through the envelope window or be visible from the outside of the envelope.

Full Social Security numbers shall not be sent through email. Simply state the individual's first and last name and last four digits of his/her Social Security number.

When it is necessary to provide a full SSN or other PII to an outside entity, e.g. an insurance company overseeing a workers' comp claim, the PII may be sent if Voltage Encryption email is utilized by La Cooperativa staff and subrecipient personnel. Do not send any emails including protected PII without using encryption software, such as Voltage.

La Cooperativa staff and subrecipient personnel shall not disclose any Social Security number over the telephone or leave a voice mail message disclosing any Social Security number. If a Social Security number must be faxed, the fax message shall be accompanied by a transmittal sheet which includes a "Confidential Notice" stating the information included is intended to be privileged and confidential and it is only intended for the use of the individual or entity named on the transmittal sheet.

All documents or files containing Social Security numbers shall be stored in a physically secure manner. Social Security numbers shall not be stored on computers or other electronic devices not secured against unauthorized access. When erasing Social Security numbers from a laptop or desktop computer, staff shall ensure the number was erased completely, including from the recycle bin.

Documents containing Social Security numbers shall not be thrown away in the trash, but instead discarded or destroyed only in a manner that protects their confidentiality, such as shredding.

This policy encompasses all programs administered by La Cooperativa Campesina de California.


ACTION:

La Cooperativa and its subrecipients shall follow this policy. This policy shall remain in effect until such time that a revision is required.

INQUIRIES:

If you have any questions regarding this Directive, please contact Marina Tapia at (916) 388-2224 or e-mail at mtapia@lacooperativa.org .

DocuSigned by:



3E7F6A7E264E4C8...

Marco Lizarraga
Executive Director