



**COUNTY OF LOS ANGELES
WORKFORCE DEVELOPMENT, AGING AND
COMMUNITY SERVICES**



CONTRACT COMPLIANCE DIRECTIVE

DATE: March 22, 2019

NUMBER: CCD 18-07

PERSONALLY IDENTIFIABLE INFORMATION DIRECTIVE

EXECUTIVE SUMMARY

The purpose of this directive is to update all Los Angeles County Workforce Development, Aging and Community Services (WDACS) subrecipients on the handling and protection of personally identifiable information (PII).

This Directive is effective on the date of release.

APPLICATION

This Directive applies to all WDACS subrecipients.

BACKGROUND

On December 26, 2013, the Office of Management and Budget revised the Uniform Administrative Requirements for Federal grants, combining those requirements with those of the audit requirements and cost principles. These regulations, which are codified at 2 CFR Chapter 1 and II, Parts 200, 215, 220, 225, and 230, became effective December 26, 2014, and are referred to as the Uniform Guidance. These rules contain requirements that Subrecipients take reasonable measures to safeguard protected Personally Identifiable Information (PII) and other information the Federal awarding agency or pass-through entity designates as sensitive or the non-Federal entity considers sensitive consistent with applicable Federal, state and local laws regarding privacy and obligations of confidentiality.

WDACS Subrecipients 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, grant and contract files and other sources. Federal regulations require that PII and other sensitive information be protected.

DEFINITIONS

PII is 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.

Contracts for Area Agency on Aging (AAA) services also includes Protected Health Information and Medical Information as part of PII.

Sensitive Information is 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.

Protected PII and non-sensitive PII - the United States Department of Labor (DOL) has defined two types of PII: (1) Protected PII and (2) 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, personal 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.

Note: The California Department of Aging states that Personal Information (PI) is information that identifies or describes an individual. PI includes but is not limited to: Name, social security number, home address, home phone number, driver's license number, medical history, as well as statements made by, or attributed to, an individual.

WDACS' AAA contracts require subrecipients to protect from unauthorized disclosure the names and other identifying information, concerning Clients receiving Program Services.

POLICY AND PROCEDURES

Subrecipients must secure transmission of PII and sensitive data developed, obtained, or otherwise associated with programs funded by WDACS and must 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. The Subrecipients must not e-mail unencrypted sensitive PII to any entity.

All Subrecipients must ensure the privacy of all PII obtained from participants and/or other individuals and protect such information from unauthorized disclosure. All Subrecipients must maintain such PII in accordance with the WDACS standards for information security described in this policy. (See Contract Sections discussing: Confidentiality – 7.6 Information Technology, Security and Privacy Requirements – 9.17, Health Insurance Portability and Accountability Act of 1996 (“HIPPA”) for detailed information. (Subparagraph number may vary with each subaward.)

Subrecipients shall ensure that any PII used during the performance of their agreement with the County has been obtained in conformity with applicable federal and state laws governing the confidentiality of information.

Subrecipients shall ensure that all PII data be stored in an area that is physically safe from access by unauthorized persons at all times.

Subrecipient employees and other personnel who will have access to sensitive/confidential/proprietary/private data (1) must be informed of the confidential nature of such information and of the safeguards required to protect such information; and (2) must be advised that, per federal and state laws, civil and criminal sanctions may be imposed for noncompliance.

As a WDACS Subrecipient, your organization is required to have in place policies and procedures under which their employees and other personnel acknowledge (1) their understanding of the confidential nature of the data, (2) the requirements with which they are required to comply when handling such data, and (3) that they may be held liable to civil and/or criminal sanctions for noncompliance with statutory nondisclosure requirements.

Subrecipients must not extract information from data supplied by automated systems including but not limited to, CalJOBS, GetCare, and Harmony for Adult Protective Services (HAPS) systems for any purpose not stated in their contract agreement with the County.

Access to any PII must be restricted to only those employees who need it in their official capacity to perform duties in connection with the scope of work in the agreement with the County.

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 may be downloaded to, or maintained on, mobile or portable devices only if the data is encrypted.

Subrecipients must ensure that the reporting package of their required organizational audits do not include protected personally identifiable information.

Subrecipients must permit county, state and federal staff 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 in this policy.

Subrecipients must retain data only for the specified period of time required to use it for assessment and other purposes, or to satisfy applicable Federal records retention requirements, if any. Thereafter, all data will be destroyed, including the degaussing of magnetic tape files and deletion of electronic data.

Subrecipients must refer to their contract Exhibit Q:

A- ACCOUNTING AND FINANCIAL RECORDS subparagraph: 3.0 Records for information on safeguarding accounting records; and

B- INTERNAL CONTROLS subparagraph 3.2 Personnel and Payroll Records Internal Controls subparagraph 3.2 for information on safeguarding personnel and payroll records.

In addition to the above, AAA Subrecipients shall refer to the following contract exhibits:
Exhibit – Subrecipient Acknowledgment and Confidentiality Agreement
Exhibit – Business Associate Agreement Under the Health Insurance Portability and Accountability Act of 1996
Exhibit - Subrecipient's Compliance with Encryption Requirements

Protecting PII

Before collecting PII or sensitive information from participants, Subrecipients must have participants sign releases acknowledging the use of PII for grant purposes only.

Note: AAA Subrecipients must have participants sign releases acknowledging the use of PII for grant purposes only. Subrecipient may allow Client to authorize the release of information to specific entities, but shall not request or encourage Client to give a blanket authorization or sign a blank release, nor shall Subrecipient accept such blanket authorization from Client.

Furthermore, all subrecipients who handle confidential information are required to complete the California Department of Aging's Privacy and Information Security Awareness Training.

Whenever possible, it is recommended that the use of unique identifiers be used for participant tracking instead of SSNs. While SSNs may initially be required for performance tracking purposes, a unique identifier could be linked to each individual record. Thereafter, 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., cross cut shredding or using a burn bag) and securely deleting sensitive electronic PII.

Subrecipients shall not leave records containing PII open and unattended.

Subrecipients shall store documents containing PII in locked cabinets when not in use.

ACTION

Subrecipients are required to take aggressive measures to mitigate the risks associated with the collection, storage, and dissemination of sensitive data including PII.

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

All WDACS Subrecipients must ensure that the requirements described herein are communicated throughout the operations, management and governance structure of their respective organization and that this Directive is adhered to until further notice.

INQUIRIES

Inquiries regarding this directive and the policies and procedures described herein should be directed to smexberry@wdacs.lacounty.gov or suraizee@wdacs.lacounty.gov.



**Paul Goldman, Assistant Director
Contracting Services Branch**