DATE: September 28, 2015

TO: LA’s Workforce Development System

FROM: Jaime H. Pacheco-Orozco, Director Workforce Development System

SUBJECT: WDS DIRECTIVE NO: 16-03 HANDLING AND PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

EFFECTIVE DATE
This directive is effective upon date of issuance.

PURPOSE
The purpose of this directive is to inform America’s Job Centers of California (WorkSource Centers and YouthSource Centers) of the City’s policy on the Handling and Protection of Personally Identifiable Information (PII).

BACKGROUND
As part of its grant activities, the City of Los Angeles Workforce Development System (WDS) 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, grant and contract files and other sources.

Definitions
- PII - 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.

- 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, 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.

Federal regulations require that PII and other sensitive information be protected. The WDS must secure transmission of PII and sensitive data developed, obtained, or otherwise associated with Workforce Innovation and Opportunity Act (WIOA) funds 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 WIOA funded agencies must not e-mail unencrypted sensitive PII to any entity.

- The City and all WIOA funded agencies 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. All agencies must maintain such PII in accordance with the DOL Employment and Training Administration standards for information security described in this policy.

- The WIOA funded agencies shall ensure that any PII used during the performance of their agreement with the City has been obtained in conformity with applicable federal and state laws governing the confidentiality of information.

- The WIOA funded agencies further acknowledge that all PII data shall be stored in an area that is physically safe from access by unauthorized persons at all times.

- The WIOA funded employees and other personnel who will have access to sensitive/confidential/proprietary/privacy 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.

- The WIOA requires that funded agencies 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 liable to civil and/or criminal sanctions for noncompliance with statutory nondisclosure requirements.

- Grantees must not extract information from data supplied by the CalJOBS / JobsLA system for any purpose not stated in their contract agreement with the City.

- 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 City.

- 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 are encrypted.

- The WIOA funded agencies must permit city, 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 WIOA funded agency is complying with the confidentiality requirements described in this policy.

- The WIOA funded agencies must retain data only for the 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.

**Protecting PII**

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

- Whenever possible, 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.

**ACTION REQUIRED**
The WIOA funded agencies 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 City, or the imposition of special conditions or restrictions, or such other actions as the City may deem necessary to protect the privacy of participants or the integrity of data.

**EWDD CONTACT**
Questions regarding this directive should be addressed to Gerardo Ruvalcaba at Gerardo.Ruvalcaba@lacity.org or (213) 744-7233, TTY (213) 744-9395.

JHP:GR:EM