Program: CWP General Policy and Procedures	**Section:** 2-20
Subject: Protecting Personally Identifiable Information (PII)	**Effective Date:** 7/1/14

Safeguarding of Personally Identifiable Information and Individual Data in Electronic Data Systems

This is an overview of the requirements governing the safeguarding of individual data stored in electronic data systems to which the employees of CWP, its subrecipients, and contractors have access. These systems store data pertaining to program participants and clients receiving services from CWP programs, through its agents, subcontractors and related entities.

General

Information concerning program participants and clients is considered confidential and may not be released or used for any purpose other than one directly connected with the administration of the program. An example of a permissible release is a referral to a service provider with information concerning the participant relevant to performing the service, such as the provision of test scores to an adult education program provider. Information may also be released when the participant authorizes disclosure.

Personally Identifiable Information (PII)

Information contained in the electronic systems to which the employees of CWP, its subrecipients, and contractors have access may contain Personally Identifiable Information (PII). PII is defined by the federal Office of Management and Budget (OMB) 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. USDOL has identified two types of PII – Protected and Non-Sensitive. The differences between protected PII and non- sensitive PII are primarily based on analysis regarding the "risk of harm" that could result from the release of the PII.

- Protected PII: Information that if disclosed could result in harm to the individual whose name or identity is linked to that information. Examples: social security numbers, credit card and bank account numbers, home telephone numbers, ages, birthdates, marital status, spouse names, educational history, biometrics (fingerprints, voice prints, iris scans, etc.), medical history, financial information, computer password, etc.

- Non-Sensitive PII: Information that if disclosed, by itself, could not reasonably be expected to result in personal harm as it is not linked or closely associated with any protected or unprotected PII. Examples: first and last names, e-mail addresses, business addresses and telephone numbers, general education credentials, gender, race, etc. However, depending on the circumstances, a combination of such items may combine 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, 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.

Any breach or suspected breach of PII must be reported to the immediate supervisor and to the CWP Compliance & Accountability Administrator.

Use of Contract Related Electronic Data Systems

Section 53a-251 of the Connecticut General Statutes contains provisions concerning computer crime. It states that a person is guilty of a computer crime if he or she accesses a computer system without authorization, accesses or causes to be accessed or otherwise uses or causes to be used a computer system with the intent to obtain unauthorized computer services, causes a disruption of computer services, damages or destroys any equipment used in a computer system, or misuses computer system information. Misuse of computer information includes the situation when a person accessing or causing to be accessed a computer system intentionally makes or causes to be made an unauthorized display, use, disclosure or copy, in any form, of data residing in, communicated by or produced by a computer system.

It is very important to not disclose a password to anyone or allow access to anyone who has not been authorized to access the system. Always log out of any of the electronic data systems to which you have access pursuant to this Contract when stepping away from your work area.

No confidential data obtained from any of these systems may be placed or stored on any mobile computing or mobile storage device.

- Mobile computing devices include but are not limited to: notebooks, laptops, palmtops, PDAs, IPods, Blackberry devices, cell phones and tablets with internet browsing capability, etc.

- Mobile storage devices include, but are not limited to: mobile computing devices, diskettes, magnetic tapes, external/removable hard drives, flash cards (e.g. SD, Compact Flash, etc.), thumb drives (USB keys), jump drives, compact disks, digital video disks, etc.

The transmission of confidential data via email is strictly prohibited.

Further Information

Questions concerning compliance with this policy may be addressed to the CWP Compliance & Accountability Administrator.