4.5 CONFIDENTIALITY AND SECURITY

Due to the confidential nature of information and documentation obtained about individuals throughout their participation in WIOA, OWD has developed the following policy in accordance with federal laws and regulations. Case managers and other WIOA Title I staff have access to personal information that must remain confidential, or that may only be dispersed to certain other entities. Every individual with access to such personal information must comply with the Family Education Rights and Privacy Act (FERPA) (20 U.S.C. 1232g) [WIOA §116(i)(3)]. Additional security measures are required for information concerning disabilities, information provided by vocational rehabilitation agencies [TEGL 7-16], and for state unemployment compensation information [20 CFR part 603].

Any person with access to personal information must read and understand the FERPA, and must receive training on the local confidentiality policy. As such, a signed confidentiality agreement acknowledging the requirements of the FERPA, in addition to the local policies and the penalties for violation of the requirements must be maintained in local files.

4.5.1 CONFIDENTIALITY POLICIES AND PROCEDURES

Local areas must develop policies and procedures to promote the security and confidentiality of personal information, which must include, but are not limited to:

- What information must be kept confidential and what information can be disclosed;
- To whom confidential information may be given;
- Manner for storing confidential information that must be maintained for reporting reasons [29 CFR 38.41(b)(2)];
- Requirement that all medical or disability-related information obtained about a particular individual must be collected on forms separate from other information collected from the individual, and treated as confidential. Whether these files are electronic or hard copy, they must be locked or

otherwise secured (for example, through password protection) [29 CFR 38.41(b)(2)], [4.5.2]

- Forms signed by individuals allowing the local area to release appropriate information to other entities that might be helpful to the participant;
- Prohibition on sensitive personally identifiable information (information that could result in harm to the individual whose name or identity is linked to the information) being electronically transmitted unless it is specifically protected by secure methodologies. Sensitive information includes, but is not limited to, place of birth, date of birth, mother's maiden name, driver's license number, biometric information, medical information (except brief references to absences from work), personal financial information, Social Security numbers (including only the last four digits), credit card or debit card account numbers, passport numbers, potentially sensitive employment information (e.g., personnel ratings, disciplinary actions, and results of background investigations), criminal history, and any information that may stigmatize or adversely affect an individual. Non-sensitive personal identifiable information that may be transmitted electronically without protection include work phone numbers, work addresses, work and personal email addresses, resumes that do not include a Social Security number or where the Social Security number has been redacted;
- Procedures for disaster recovery of paper and electronic information;
- Prohibition on confidential information being discussed or disclosed in telephone conversations unless it is certain that the other party has authorized access to the information; and
- Requirement that paper documents must be secured in a manner so that unauthorized access (such as by individuals walking into the room) is unlikely.

The policies and procedures are also encouraged to include the following:

- Penalties for misuse, mishandling, or unauthorized disclosure or confidential information;
- Statement that information may be disclosed only on a "need to know" basis;
- A process for individuals who request that normally-public information not be disclosed (for example, address of a person who is escaping an abusive ex-spouse);
- Requirement that computers may be used for business use only;
- Regulations concerning the security of laptop computers when not in use, when taken home, and when traveling;
- Requirement that all computers must be password protected;
- Requirement that all computers must have screen savers with password protection or keyboard locking program activated on them;
- Requirement that the use of the internet is confined to official business only;
- Prohibition on downloading or installing any software or program without consent;
- Requirement that all servers must contain anti-virus software that is updated automatically;
- Notice that the use of network activity may be monitored without an employee's knowledge or consent;
- Requirement that computer monitors must be positioned such that unauthorized viewing is unlikely;
- Requirement that a confidentiality notice must be added to all email messages;
- Requirement of background checks for individuals with access to confidential information;
- Prohibition on recording telephone conversations without the consent of the individuals being recorded; and
- Requirement that documents and papers containing confidential information must be shredded personally or taken to a secure storage place to be shredded.

4.5.2 STORAGE OF CONFIDENTIAL INFORMATION

Any information collected from an applicant regarding a medical examination or through inquiries regarding a disability (as defined by 29 CFR 38.4), or other information regarding the medical condition or history of an applicant, must be kept confidential and separate from the individual's application. All LWDAs must take steps to guarantee the security of such information.

Additionally, LWDA employees' medical information must be kept in a separate location from other employment or training records. These files must be kept in a medical file in a separate locked cabinet apart from the location of other personnel or training files.

In accordance with 29 CFR 32.15(d) and 29 CFR 38.41(b)(3), all records containing medical or disability related information, including information relating to an individual's disability status, must be:

A. Collected on separate forms and kept in separate files, apart from all other information about a particular individual;
B. Stored securely, with limited access (e.g., electronic files password protected, hard files kept locked); and
C. Available only to persons with a need to know, as provided in 29 CFR 32.15(d) and 29 CFR 38.41(b)(3).