

---

## Western Arkansas Workforce Development Area Policies and Procedures

---

<b>TITLE</b>	Personally Identifiable and Confidential Information
<b>NUMBER</b>	P0004-24
<b>TYPE</b>	Policy - Operations
<b>APPROVING AUTHORITY</b>	Western Arkansas Workforce Development Board
<b>EFFECTIVE DATE</b>	4/30/24
<b>NEW/REPLACED</b>	P#0008-18 & P0003-23

### **Background**

As Workforce Innovation and Opportunity Act (WIOA) or other funded services are provided through a customer-centric case management system, staff obtain personal and confidential information from individuals to the extent allowed for State and Federal Law in order to facilitate an individual's access to services. This confidential information may be shared among the partner agencies of the workforce system.

In accordance with Federal and State Law, individuals applying for the WIOA, or other funded services must be provided an opportunity to submit written authorization allowing the service provider to share their personal and confidential information and records. Each individual must also be informed that they can request their personal and confidential information not be shared among the partner agencies of the workforce system and this request does not affect their eligibility for services. If an individual declines to share their personal and confidential information and is eligible for and receives services, Western Arkansas will work with the State to identify a pseudonym to document the participant's program services.

### **Policy**

1. It is the policy of the Western Arkansas Workforce Development Board to protect and safeguard personal and confidential information provided by individuals seeking Workforce Innovation and Opportunity Act or other funded services. Individuals seeking services must be informed, in writing via the Authorization to Share Confidential Information and Records Form, that their personal and confidential information:
  - a. May be shared among the local workforce system partner staff and sub-contractors;
  - b. Is used only for the purpose of delivering services and that further disclosure of their confidential information is prohibited; or,
  - c. Will not be shared among partners of the local workforce system if the individual declines to share their confidential information and the decline to share will not impact their eligibility for services.
2. To protect PII (personally identifiable information) of clients the following procedure is enacted as required by ETA/DOL and noted in TEGL 39-11. These procedures also ensure trackability of client files.
  - a. Upon receipt of a client application a file will be created or updated and secured in the file room.
  - b. ALL files and documents containing PII must be secured in the file room. The exception is when a staff member is working on the file. When staff is not

---

## Western Arkansas Workforce Development Area Policies and Procedures

---

- immediately working on a file it is to be secured in the file room including overnight, weekends and holidays. Any PII received or scanned to a computer or temporary storage must be expediently placed in the appropriate file and promptly deleted from any non-designated site.
- c. To maintain track of files, a sign in and out sheet has been created and will be maintained in the file room. This is to ensure files can be located any time.
  - d. To make this manageable for all staff, a file cabinet has been designated and marked for in-process files. This cabinet can be used to place in-process files in your designated drawer or in the appropriate program file drawer.
3. Whether written or oral and regardless of format, staff must maintain confidentiality of the following:
- a. Information that was created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse. This includes any case notes, chart entries, or treatment notes that relate to health information.
  - b. Information that is related to an individuals' physical or mental health or medical condition in the past, present, or future; healthcare provided or to be provided to an individual; or payment for healthcare provided to an individual in the past, present or future.
  - c. Information that identifies an individual, employee, or participant.
4. The misuse or unauthorized release of personal and confidential information or records by any WIOA service provider and staff may be subject to a civil penalty and other applicable sanctions under applicable State and Federal Law.
5. Every individual receiving WIOA, or other services must read, sign and date the Authorization to Share Confidential Information and Records form.
6. Every individual receiving WIOA, or other services must be informed of their right to not share their personal and confidential information and that this request does not affect their eligibility for WIOA services.
7. Medical and Disability Information: Personal and confidential information that contains health information related to a physical or mental disability, medical diagnosis or perception of a disability related to the individual must be kept in a separate locked file and apart from working files.
8. Any medical information contained in case notes must be redacted from the participant file; the original notes must be placed in participant's medical file.
9. To minimize the need for staff to access a medical file, only the portion of the participant's information that reveals the presence of a disability should be included in the medical file.
10. Access to the medical files:
- a. Must be limited and should only be accessed with the approval of program management and when such access is necessary to facilitate a WIOA participant's access to services or to support an ongoing service plan; or,
  - b. First aid and safety personnel may be provided participant medical information in the event of an emergency; or,
  - c. Local, State, or Federal monitors in compliance with 29 CFR 32.44(c) and 29 CFR 38.60 may have access to medical files for monitoring purposes.

---

## Western Arkansas Workforce Development Area Policies and Procedures

---

11. When all services, including follow-up services, are complete and the participant file is ready to be archived, participant medical and disability-related information that had been previously filed away from the active file must be placed in a sealed envelope and marked “Medical and Disability Information” and secured in the participant file.
- a. Archive boxes must be clearly marked as containing personal and confidential information.
  - b. Staff should avoid communicating personal and confidential information about an applicant/participant to partner agencies of the workforce system via email. If it is absolutely necessary, staff must ensure that the recipient is the only person who has access to the information and that the recipient understands they also must protect the information. Further, participant information must only be communicated through agency approved email addresses and not through third party or personal email addresses.
  - c. Social security numbers may not be delivered through email. Staff should discourage participants from emailing personal and confidential information, such as social security numbers, to workforce staff. However, in the event a staff person receives participant confidential information via email, the staff person should immediately delete the email and subsequently delete the email from the “deleted items” folder.
  - d. Staff should be discreet when verbally communicating personal and confidential information and ensure the receivers are authorized to receive the information.
  - e. Staff must not leave personal and confidential information lying out in the open and unattended. Personal and confidential information must be stored in a secure location when not in use or shredded if no longer necessary. Personal and confidential information should not be tossed in the regular trash or recycle bins.
  - f. Staff must ensure that they have logged out of any online application that contains the participant’s name, etc. (i.e. AJL) when away from desk.

---

**Approval Signature:**

John Craig, Board Chair