ARIZONA@WORK™
Innovative Workforce Solutions
A proud partner of the americanjobcenter network

Personally Identifiable Information (PII) Resource Guide

ARIZONA@WORK collects personal information, also known as Personally Identifiable Information (PII). As an employee, service provider, or contractor, you are required to protect this PII in accordance with the policies of the Department of Labor (DOL) and the Department of Economic Security (DES/DERS). It is essential to safeguard this information to prevent identity theft and other negative outcomes, such as privacy incidents, data compromises, or misuse of data.

It is imperative to exercise care when handling all PII. This resource guide provides best practices and policy requirements to prevent a privacy incident involving PII during all stages of the data entry and information life cycle.

This Resource Guide explains:

- how to identify PII;
- how to protect PII in different contexts and formats; and
- what to do if you believe PII has been lost or compromised.

Why is PII Important in the WIOA (Workforce Innovation and Opportunity Act) System?

PII is essential for tracking participants' progress, ensuring compliance with federal regulations, and providing targeted services. It helps WIOA programs:

- Identify eligible participants
- Develop individualized service plans
- Monitor participant outcomes
- Report data to federal and state agencies

Common data elements used as PII for Data Validation:

- Drivers License
- Baptismal Record
- Birth Certificate
- DD-214
- Report of Transfer or Discharge Paper
- Federal, State, Local or Tribal Identification Card
- US Passport
- Hospital Record of Birth
- Public Assistance/Social Service Records
- School Records or ID Cards
- Work Permit
- Family Bible
- Cross-match with State Agency Records
- Justice System Records
- Selective Service Registration
- Signed Letter from a parent or guardian
- Medical Records
- Self-Attestation

Best Practices for Entering PII

1. **Verify Accuracy:** Always double-check the accuracy of all PII before entering it into the system. Errors can lead to delays in services and potential privacy breaches.
2. **Protect Data:** Ensure that the WIOA system has robust security measures in place to protect PII from unauthorized access.
3. **Limit Access:** Restrict access to PII to authorized personnel only.
4. **Train Staff:** Provide staff with training on proper handling and storage of PII.
5. **Comply with Regulations:** Adhere to all federal and state regulations regarding PII.

Additional Guidelines to minimize the use of PII when possible:

1	Limit access to PII to only staff who need such access.
2	Include processes for retaining and destroying documents with PII.
3	Avoid the need to remove documents with PII from secured areas.
4	Lock computer screens when not in use.
5	Use encrypted devices.
6	Password-protect files with PII.
7	Double-check email before sending PII, email must be sent secure or encrypted.

By following these guidelines, you can help ensure the secure and responsible handling of PII in the WIOA system.

How to redact PII:

Manual Redaction:

- **Use a black marker or red pen:** Physically cover the sensitive information.
- **Use white-out:** Apply white-out to the sensitive information. *(Whiteout should only have limited use as it may appear to tamper with the authenticity of the document)*.

Digital Redaction:

- **Use PDF Redaction Tools:** Many PDF editors have built-in redaction tools. Be very cautious to ensure the redaction is permanent on any file that is uploaded.
- **Use Image Editing Software:** Tools like Adobe Photoshop can be used to black out sensitive information in images.
- **Use Specialized Redaction Software:** There are software tools designed specifically for redacting sensitive information.

Tips for Effective Redaction:

- **Be thorough:** Ensure that all sensitive information is redacted.
- **Be precise:** Redact only the necessary information.
- **Be consistent:** Use a consistent redaction method.
- **Verify the redaction:** Double-check your work to ensure that no sensitive information is visible.

By following these guidelines, you can help protect sensitive information and prevent data breaches.

WIOA Data Elements

The Workforce Innovation and Opportunity Act (WIOA) aims to improve workforce development systems in the United States. It emphasizes the need for data collection and reporting to evaluate program effectiveness.

Key Data Elements:

WIOA requires states to collect and report specific data elements related to individuals served by workforce programs. When collecting WIOA Data Elements staff need to be aware that some of the data could be PII.

Below are some examples of key data elements and their significance, however this is not an exhaustive list:

1. **Demographic Information:**
   - Name: Identifies the individual.
   - Social Security Number: Unique identifier for tracking services and outcomes.
   - Date of Birth: Used for age-related analyses.
   - Gender: Important for understanding service demographics.
2. **Program Participation:**
   - Program Enrollment Date: Date the individual enrolls in a WIOA program.
   - Program Exit Date: Date the individual exits the program.
   - Service Types Received: Details on the specific services provided, such as training or career counseling.
3. **Employment Outcomes:**
   - Employment Status Post-Exit: Whether the individual is employed, unemployed, or not in the labor force after exiting the program.
   - Wage Information: Earnings of the individual post-exit to assess the effectiveness of the program.
4. **Education and Training:**
   - Highest Education Level Completed: Educational attainment for analyzing program impacts.
   - Training Services Received: Specific training programs or certifications obtained.
5. **Barrier Information:**
   - Disability Status: Whether the individual has a disability, which helps in assessing service accessibility.
   - Basic Skills Deficiency: Information on individuals who may require additional support for skill development.

Reporting Requirements:

- States are required to submit periodic reports that include aggregate data on these elements, which helps in evaluating workforce program effectiveness and improving services.

Compliance and Security

Data Protection Regulations:

- Ensure compliance with federal and state regulations regarding PII protection, including but not limited to:
- FERPA (Family Educational Rights and Privacy Act)
- HIPAA (Health Insurance Portability and Accountability Act)

Secure Data Management:

- Implement secure systems for data storage and transmission, including the use of filters to prevent mistakenly sending PII.
- Regularly audit data access and handling practices.
- Require staff to take regular security training, this is the best way to prevent a breach or mistaken disclosure.

Conclusion:

Protecting PII while effectively utilizing WIOA data elements is essential for both compliance and the success of workforce programs. By adhering to best practices and understanding the importance of these data elements, organizations can improve their service delivery and protect the privacy of individuals.

Additional Resources

- U.S. Department of Labor WIOA Resources: [DOL WIOA] (https://www.dol.gov/agencies/eta/wioa/guidance)
- National Institute of Standards and Technology (NIST) Guidelines on II: [NIST PII Guidelines] (https://csrc.nist.gov/publications/detail/sp/800-122/final)
- DOL Data Protection: (https://www.ecfr.gov/current/title-29/subtitle-A/part-71/subpart-A/section-71.1)
- DOL Training and Employment Guidance Letter (TEGL) 39-11
- DOL Training and Employment Guidance Letter (TEGL) 7-18
- DOL Training and Employment Guidance Letter (TEGL) 23-19, Change 2

ARIZONA@WORK™

Innovative Workforce Solutions

A proud partner of the americanjobcenter network

Equal Opportunity Employer / Program • Auxiliary aids and services are available upon request to individuals with disabilities • To request this document in alternative format or for further information about this policy, contact your local office; TTY/TDD Services: 7-1-1

WIO-1269A PAMENG (01/25)