Personally Identifiable Information
Policy #P-3-3.22

Date: August 8, 2022
Re: Handling and Protection of Personally Identifiable Information (PII)

Approved: March 24, 2022
Effective: March 25, 2022

References: TEGL 39-11
TEGL 05-08
29 CFR Part 32.44(c)
29 CFR Part 38.60
42 CFR Part 2

Author: Saranne Miller, SCPa Works Policy Manager

Attachments: PII Sign-Off Form
PII WIOA/TANF Participant Consent to Release Information Form

I. Background:

A. All grantees are required to protect PII sensitive information (as defined in TEGL 39-011 and includes, but is not limited to, SS#, birthdates, financial/education information, etc.) when collecting, storing and/or disposing of information. The following content has been implemented to uphold this policy in order to ensure that WIOA/TANF participant PII is not accessible to any unauthorized individuals including other customers, email recipients, or cleaning crews.

II. Purpose:

A. All grantees that have access to sensitive, confidential, proprietary, private data, or other PII must maintain the confidential nature of the information and the safeguards required to protect the information.
B. Failure to maintain confidentiality may result in civil and criminal sanctions for noncompliance. Such safeguards that are contained in federal and state law and South Central Workforce Development Board (SCWDB) policies must be strictly followed.
    1. All staff must comply with TEGL 39-11 and associated Appendix: Applicable Federal Laws and Policies Related to Data Privacy, Security and Protecting Personally Identifiable and Sensitive Information, which contains guidelines for handling such PII data.
    2. Failure to comply with TEGL 39-11 may result in civil and criminal sanctions for improper disclosure.
    3. PII data shall not be extracted from client files whatsoever and for any reason or purpose except with the approval of the SCWDB.

4. PII data supplied to the grantees by the SCWDB or ETA, or any other federal or state funded program, shall not be extracted for any purpose not stated or authorized in the associated grant or funding authority agreement.
5. Any WIOA/TANF participant PII data either collected or created must be restricted only to those employees who need it in their official capacity to perform their duties as grantees.

III. Paper Documentation:

A. Records containing PII are not to be left opened and unattended.
B. All paperwork containing PII must be secured in locked file cabinets that are physically safe from access by unauthorized persons at all times.
C. Security is to be maintained when transporting files.
D. Unless otherwise required, files containing PII must remain in designated locations approved by the SCWDB.
E. Use of the Participant Identification (PID) number is required whenever possible, not the SSN.
F. Any paperwork containing PII must be disposed of by using a cross-cut shredder or approved shredding service.
G. Participant files that have been exited are to be kept in either locked file cabinets, or storage rooms/facilities that are secured by lock.
H. Files and participant data shall only be retained for the period of time required to use the information for assessment and other purposes, or to satisfy applicable federal and local records retention requirements.

IV. For Data Contained on Computer Drives and Other Hardware:

A. All PII data regarding clients obtained through any and all grants will remain stored in areas that are physically safe from access by unauthorized persons at all times.
B. Data files containing PII must remain in designated locations approved by the SCWDB.
C. Accessing, processing, and storing of PII data on personally owned equipment, or at off-site locations (including an employee's home), and other unauthorized services (public email systems), is strictly prohibited unless approved by the SCWDB.
D. To ensure that such PII is not transmitted to unauthorized users, all PII and other sensitive data transmitted via e-mail or stored on CD's, DVD's, thumb drives, etc. must be encrypted using a Federal Information Processing Standards (FIPS) 140-2 compliant and National Institute of Standards and Technology (NIST) validated cryptographic module.
E. Grantees must not email unencrypted sensitive PII to any entity, including ETA or contractors.

V. Additional Restrictions:

A. As determined necessary by the SCWDB management, grantees may be required to use external systems to successfully conduct day to day operations.
    1. Where PII is being shared, transferred, obtained, or stored, all SCWDB PII policies and procedures must be strictly maintained, and where dictated by the external system authorizing agent agreement, any additional PII requirements must also be strictly adhered to.
B. All grantees must safeguard PII as part of their daily actions and work routines.
C. PII is defined as any information on clients that can be used to identify or expose them to risk of identity loss including social security numbers, dates of birth, and financial and educational records.
D. For authorized personnel, PII is made available on a need-to-know basis when required. For all other personnel, access to such information is prohibited.
E. Unauthorized modification, transmitting or other dissemination of PII is strictly prohibited.
F. PII must be safely stored and protected while on file servers, network drives, workstations, and during any type of transmission.

1. PII should be erased securely from network drives, file shares, etc. after proper authorization.
2. Network or directory share information showing where the PII is stored must not be publicly viewable.
3. PII must not be emailed unless the grantee is setup with email encryption and thus authorized to transmit such data.
4. Grantees without email encryption are forbidden from sending any PII whatsoever.
5. Grantees must not download and store confidential information unless encrypted on their personal computers.
6. Storage of PII on anything other than an encrypted computer is expressly forbidden. This includes all CD/DVD, USB drives, and any other external storage devices.

G. Printed documents that contain PII must not be left available to the public. All printed PII that is not included in a participant's physical case record file must be shredded or properly disposed.
H. Employees must not take printed or unencrypted PII home.
I. Employees must not discuss PII in public.
J. The IT department can monitor any employee's email and computer at any time to ensure compliance with the above in regards to storage and transmission of PII.
K. All participant data or any data that contains PII must be sent using secure email, data encryption, or through a secure document repository. When requesting data that contains PII, SCPa Works may instruct respondents to use a particular, secure method of transmission. SCPa Works is required to report any possible data breaches to the State Department of Labor & Industry, and may impose sanctions on any contracted entity, organization, and service provider that transmits PII via unsecure means.
L. Violations of or failure to follow this policy and its procedures shall result in corrective action as determined by the SCWDB.

VI. Medical and Disability Information:

A. Whether written or oral and regardless of format, staff must maintain the confidentiality of the following:
    1. 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.
    2. 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 contained in case notes **must be redacted** from the participant file; the original notes must be placed in the participant's medical file.
B. Access to the medical files:
    1. Must be limited and should only be accessed **with the approval of program management** and when such access is necessary to facilitate a participant's access to services or to support an ongoing service plan; or
    2. First aid and safety personnel may be provided participant medical information in the event of an emergency; or
    3. Local, state, or federal monitors in compliance with 29 CFR Part 32.44(c) and 29 CFR Part 38.60 may have access to medical files for monitoring purposes.
    4. When a request for medical records is initiated, a WIOA/TANF participant must sign and date SCPa Works Consent to Release Information form.
        a. This signed form will be maintained in the participant's physical case record file.
C. 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

separately from the active file must be placed in a sealed envelope and marked, "Medical and Disability Information."

1. The sealed "Medical and Disability Information" will be secured in the participant file.

VII. Sign-Off Form Procedure:

A. All SCPa Works, PA CareerLink®, and contracted service provider staff members authorized to safely handle PII must sign the PII Sign-Off form.
B. All staff affiliated with WIOA/TANF service delivery, administration, and operations will comply with the PII Procedures to ensure PII protection while delivering services to participants in a local office or within a community-based facility.
C. All service provider staff will alert program managers when PII is discovered out of place, missing, or stored in an unlocked, unsupervised cabinet, desk, or storage area.

VIII. Participant File Protection:

A. Participant Files will stay in appropriate CareerLink® comprehensive sites.
B. Staff will scan PII documents and store them on the computer versus transporting the documents and will use electronic signature equipment to drastically reduce and eventually eliminate the need for printing and transporting.
C. Exceptions to this policy will be reviewed on a case-by-case basis and granted in writing by a service provider program manager.
D. When an exception is granted and a file must be transported by service provider staff, the following measures must be taken:
    1. Participant files and additional documents containing PII may only be transported in a visibly locked box designated by the service provider for mobile operations.
        a. No other methods of paper file protection will be recognized as compliant with this procedure.
    2. A file check-out and tracking form will be created by the service provider, completed, signed by the site administrator, and left in place of the file in the original file location.
    3. The file transport must be tracked on a document control summary form created by the service provider, signed by the site administrator, and easily accessed by other staff at the file's original comprehensive site.
    4. When the file is returned, the file check-out and tracking form may be removed from the original file location, signed by the site administrator, and filed with the document control summary form.
    5. The return of the file must be acknowledged on both the check-out and tracking form and the document control summary, with all signatures in place.

IX. Confidential Interaction:

A. WIOA/TANF staff will be cognizant of the fact that verbal confidential conversations occur in public spaces to include PII content and sensitive information relating to participants.
    1. Staff members will ensure discretion is used at all times.
    2. Methods of employing discretion in a public setting include keeping voices at a low volume or pointing to, writing, or typing sensitive information instead of speaking it aloud.

X. Technological Security:

A. WIOA/TANF staff will utilize secure operating systems, computers, printers and scanners while working with participants in the community.
    1. Any type of equipment that is utilized to administer WIOA/TANF services to participants will not be left unattended and/or available for unauthorized use.

2. Staff members will not share passwords.
3. If equipment is missing, please report the product, equipment ID#, and a description of the missing items to the service provider manager immediately.

XI. Definitions:

A. PII: Any 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.

B. Sensitive Information: Any unclassified information whose loss, use, misuse, or unauthorized access to or modification could adversely affect the interest or the conduct of Federal programs, or privacy to which individuals are entitled under the Privacy Act of 1974.

C. Protected PII and Non-Sensitive PII: 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, voice prints, 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, email addresses, business addresses, business telephone numbers, general education credentials, gender, or race.
    a. 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 email 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.

D. Authorized Personnel: Any staff person working for a WIOA/TANF service provider or organization contracted under SCPa Works who has signed the PII Sign-Off Form and has received authorization from WIOA/TANF service provider leadership or organization management to handle and/or manage PII in accordance with SCPa Works' PII policy #P-3-3.22. Staff members under this definition can include, but are not limited to, staff assigned to positions within a PA CareerLink®.

E. Security Breach: A term used to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.

XII. Summary of Changes: This policy is reviewed every 180 days by the SCPa Works Policy Department for necessary changes, edits, updates, and revisions.

Date of Change:	Changed by:	Summary of Change(s):	Effective Date
03/15/2022	Saranne Miller	Reformatted in 2022 policy template. Added citations and definitions.	03/15/2022

		Added PII SOP.	
08/04/2022	Saranne Miller 	Removed form ID numbers from the Attachments header and throughout the policy. Updated approval dates on policies and forms. Adjusted signature line formatting on forms. Edited footer to reflect current policy approval date. Reformatted Section XI. Revised language to include TANF guidance. Combined PII Procedures with the body of the policy and removed Procedures from the Attachments header. Reviewed all documents for updates; no further updates were necessary.	08/04/2022