Advance Central PA
Linking People & Business

Confidentiality and Personal Identifiable Information Policy

Approved by the Central PA WDB September 18, 2019

Developed by:
Central Pennsylvania Workforce Development Corporation, dba Advance Central PA

Advance Central PA Confidentiality and Personal Identifiable Information Policy

Background

Strong, effective security of Personal Identifiable Information (PII) is required at all times, including in regard to case file management, transport, electronic storage, and communication. PII is defined 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. Failure to correctly identify and protect PII could result in the loss of service, loss of state or federal funding, or present the risk of legal and financial repercussions.

The Department of Labor and Industry has defined two types of PII: Protected PII and Non-sensitive PII. The differences between 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.

- **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, voiceprints, iris scans, etc.), medical history, financial information and computer passwords.
- **Non-Sensitive PII** is information that, if disclosed by itself, will likely not result in personal harm. Essentially, it is stand-alone information that is not linked or closely associated with any Protected PII. Examples of Non-sensitive PII are first and last names, e-mail addresses, business addresses, business telephone numbers, general education credentials, gender, or race.

Depending on the circumstances, a combination of Non-Sensitive PII could potentially be categorized as Protected PII. To illustrate the connection between Non-sensitive PII and Protected PII, the disclosure of a name, business e-mail address, or business address is not likely to result in a high degree of harm to an individual. However, a name linked to a Social Security Number (SSN), a date of birth, or mother's maiden name could result in identity theft.

It is the intent of the Advance Central PA to take all necessary steps to protect PII, therefore anyone working under the Workforce Innovation and Opportunity Act, Department of Human Services EARN programming, and other funding from Advance Central PA and the Pennsylvania Department of Labor and Industry is required to protect and secure PII at all times.

Securing PII

Protection and security of PII is required at all times, including when transmitting information, collecting, storing and/or disposing of information. All PII must be processed in a manner that will protect the confidentiality of the records/documents and prevent unauthorized persons from retrieving such records by computer, remote terminal or any other means.

Requirements

1. PII shall be stored in an area that is physically safe from access by unauthorized persons at all times; all paperwork with PII must be secured in locked file cabinets when not in use.

2. Case files and documentation with PII must not be left in an open area such as a desk top even when attended by staff if the staff is working with another individual.
3. Staff computers must be locked at all times when unattended; when meeting with customers, staff computers must not have files with PII for other individuals open on their computers.
4. Participant IDs should be used in place of SSNs and other PII in all cases where SSNs are not required. Although Participant IDs with names are not considered protected PII, they should still be kept from public view within work areas.
5. All emails containing PII must be sent using encryption.
6. SSNs must never be emailed unless it is required by the recipient agency, in which case password protection and use of the appropriate secure email system is required (for example, the Unemployment Compensation (UC) Center requires use of SSNs).
7. Incoming information which includes PII must be handled to ensure security and confidentiality.
8. No individual's case file should contain any class rosters or other information containing names and/or PII of other individuals.
9. The main case files shall not include identifiable health care information. A separate case file that houses such necessary information shall be maintained with the strictest of confidentiality in accordance with the Health Insurance Portability and Accountability Act (HIPAA) and 29 C.F.R. 38.41(b)(3) which states that any medical or disability-related information must be collected on separate forms and maintained in separate confidential files.
10. Knowledge of disability status or medical condition and access to related information must be adhered to in accordance with 29 C.F.R. 38.41(b)(3) so that confidentiality is maintained and reasonable accommodations are made.
11. Staff will not ask for PII from any customer where it can be heard by other customers in the PA CareerLink® or is viewable to the public. Confidential information, such as names, addresses, and social security numbers, must not be viewable by anyone other than necessary parties within the PA CareerLink®.
12. An individual's confidential information kept on file at the PA CareerLink® may not be released to outside parties unless the individual has granted written consent to release such information.
13. Staff will restrict access to any PII through program and grant activity to only those employees who need it in their official capacity to perform duties within the scope of work in the grant agreement.
14. Information obtained from the job seeker and from other sources in regard to the job seeker is confidential and will be maintained as such.
15. When disposing of any documents that contain PII, the documents must be destroyed (shredded) prior to recycling so that the information is no longer identifiable.
16. Referrals and sharing of information to partners are allowable after written consent from an individual is granted and must be done in a manner consistent with protection of PII.
17. Advance Central PA's secure SharePoint site may be used as a secure means of sharing customer information with other authorized PA CareerLink® staff who have access to the site.

18. Files must not be downloaded unless absolutely necessary, and if so, the files must be saved to the secure server and never saved to the Downloads folder on the hard drive.
19. Any files with PII must be stored on the secure server at all times; they must never be stored on a local drive/hard drive.
20. Any paperwork with PII that needs to be scanned should be scanned directly to the server using capabilities set up on the scanning device. Note the server folders are visible to other staff members, so immediately after the file is scanned, it should be moved from the scan folder to another folder on the secure server.
21. Staff will regularly check public computers to:
    a. Determine if there are any personal files that were saved by the customer and if so, promptly remove them
    b. Determine if the customer has logged out of all internet sites such as pacareerlink.pa.gov and do so as necessary
    c. Reset to the home page
22. Files that contain PII should never be opened on a home computer or other device that is not on the secure network.
23. PII should never be accessed in public places outside of the secure network.

Transport of Case Files and Other Documents with PII

Taking case files and other records off-site should only happen when it is a necessity to do so and there is no alternative method for accessing or recording the information required. When PII, whether electronic or within paper records, is taken off-site, it should be kept to a minimum both in terms of content and duration.

When records are in transit from one location to another, they should be transported in a way that mitigates against the risk of theft or loss. Locked file boxes should be used. Loose papers should not be carried.

Chain of Custody

When records are transferred from one party to another, a chain of custody will show the reason for transfer, the name of the person transferring, the name of the person receiving, signatures and dates with copies for both parties.

The Link

Storage and security of The Link is the responsibility of the Subrecipient as well as any partner staff while working from The Link. The Link will be locked at all times when not in use and will be parked in a safe location.

Confidentiality and security of all PII on The Link is held to the requirements listed within this policy. In addition, the following specific protocols will mitigate a security breach in a mobile environment.

1. Screen shields will be used on all computer monitors to protect individuals who are registering on PA CareerLink® or doing other work involving use of PII from having their computer screens visible to others.

2. Staff computers will be locked at all times they are not physically in use by the staff person.
3. Any information with PII must be inaccessible to anyone but authorized staff, must be securely locked in a cabinet when not in use, and shredded after no longer needed and/or entry in CWDS is complete.
4. **Immediately** after a customer is finished using a public computer staff will:
    a. Determine if there are any personal files that were saved by the customer and then promptly remove them
    b. Determine if the customer has logged out of all internet sites such as pacareerlink.pa.gov and do so as necessary
    c. Reset to the home page

Removable Media

Removable media includes thumb drives, USB drives, flash drives, SD storage, and any other portable media storage unit that has information accessible by connecting to a computer. In order to mitigate risk of malware and risk to the network and sensitive information therein, removable media that did not originate from and stay within staff possession at all times is prohibited from use on staff computers.

PA CareerLink® customers may present with removable media that has information such as a draft resume; they may only access the information on their removable media using a computer designated for the public.

Staff use of removable media for any level of PII or other sensitive information is expressly prohibited.

Data Sharing

Per the MOU, the Central PA CareerLink® network partners agree that the collection, use, and disclosure of customers' personally identifiable information (PII) is subject to various requirements set forth in Federal and State privacy laws. Partners acknowledge the execution of the MOU, by itself, does not function to satisfy all of these requirements.

All data, including customer PII, collected, used, and disclosed by Partners will be subject to the following:

- Customer PII will be properly secured in accordance with the Local WDB's policies and procedures regarding the safeguarding of PII.
- The collection, use, and disclosure of customer education records, and the PII contained therein, as defined under FERPA, shall comply with FERPA and applicable State privacy laws.
- All confidential data contained in UI wage records must be protected in accordance with the requirements set forth in 20 CFR part 603.
- All personal information contained in VR records must be protected in accordance with the requirements set forth in 34 CFR 361.38.

- Customer data may be shared with other programs, for those programs' purposes, within the PA CareerLink® system only after the informed written consent of the individual has been obtained, where required.
- Customer data will be kept confidential, consistent with Federal and State privacy laws and regulations.
- All data exchange activity will be conducted in machine readable format, such as HTML or PDF, for example, and in compliance with Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. § 794 (d)).

All PA CareerLink® and partner staff will be trained in the protection, use, and disclosure requirements governing PII and any other confidential data for all applicable programs, including FERPA-protected education records, confidential information in UI records, and personal information in VR records.

Security Breach

A PII breach is defined by the Pennsylvania Breach of Personal Information Notification Act. In general, a breach is the unauthorized access and acquisition of data that materially compromises the security or confidentiality of personal information.

Advance Central PA and the PA CareerLink® Operator will be notified without delay and no more than 24 hours after a breach or suspected breach is known.

If a breach is determined, all required state and federal laws and mandates related to remediation and notification will be strictly adhered to.

Agreement

In addition to all other information in this policy, the following shall be strictly adhered to and understood.

Confidentiality obligations will survive the expiration or termination of employment and/or internship with any entity.

Staff shall use any personal and confidential information provided solely for the purpose for which the information was disclosed. Staff shall not disclose or misuse any personal and confidential information unless disclosure is authorized by law.

Staff may not use for personal gain confidential information obtained as a result of service or employment; neither may employees use such information in any way which is inconsistent with the fair and impartial conducting of business.

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires that organizations protect identifiable individual health care information. Staff will abide by security requirements and obligations, and acknowledge they are bound by confidentiality provisions. All individual health care information is to be treated as protected PII and in accordance with HIPAA.

There will at all times be adherence to all governing guidelines including federal law, OMB guidance, United States Department of Labor, Employment and Training Administration policies as well as any other relevant state and local requirements, including the following.

- Workforce System Policy (WSP) No. 03-2015 Financial Management Policy
- L&I, Office of Information Technology Policy Security SEC-001
- Training and Employment Guidance Letter (TEGL) 39-11

- Health Insurance Portability and Accountability Act (HIPAA)
- Management Directive 205.34 Amended
- Pennsylvania Breach of Personal Information Notification Act

Nothing in this clause is to be construed as blocking responsibility to assist Advance Central PA or a federal or state agency in conducting an audit or an evaluation.

Policy Acknowledgement

This Advance Central PA Confidentiality and PII Policy is widely disbursed via email to the PA CareerLink® Operator and Administrators, and is saved to the Advance Central PA SharePoint website for ready access.

All staff operating under Title I of the Workforce Innovation and Opportunity Act, Department of Human Services EARN programming, and other programs funded by grants from Advance Central PA will read and adhere to this policy.

Any and all questions should be submitted to Advance Central PA. Upon understanding of the policy, a signed acknowledgement will be documented using the attached form. Advance Central PA subcontractors will ensure all current staff sign acknowledgement within 30 days of policy release and/or within the first week of employment and submit to Advance Central PA.

Attachment A

Advance Central PA Confidentiality and PII Policy Acknowledgement Form

In effect: September 18, 2019 until further notice

I acknowledge I understand the Advance Central PA Confidentiality and Personal Identifiable Information (PII) Policy. I have received a copy of the policy and carefully read it and know how to access it going forward. I have asked any questions I may have had and acknowledge understanding of the content, requirements, and expectations and will abide by the policy guidelines which extend indefinitely beyond my current employment.

I understand that if I have questions at any time regarding the Advance Central PA Confidentiality and PII Policy, I will consult with my immediate supervisor or Advance Central PA.

Printed Name: _____

Employer of Record: _____

Signature: _____

Date: _____

Immediate Supervisor Signature: _____

Date: _____