Union County
Protection of Personally Identifiable Information (PII) Policy

1. Purpose

To provide guidance to all Union County Workforce Development partners regarding the handling and protections of personally identifiable information (PII). Compliance with these requirements will be monitored by the Union County WDB. Any noncompliance with the requirements provided in this guidance is subject to corrective action.

2. References

- 20 CFR 683.220; Training and Employment Guidance Letter 39-11
- §200.82 Protected Personally Identifiable Information (Protected PII)
- §200.303 Internal controls.
- NJ LWD TEGL 39-11

3. Background

The Union County Workforce Development Board (WDB) and the American Job Centers (AJC) within Union County are committed to protecting the customer's right to privacy. The WDB and the AJC, referred to as the Union County Workforce Partnership (Workforce Partners), value and protect the customer's privacy and place strict controls on the gathering and use of personally identifiable data. Personal information is not disclosed, made available, or otherwise used for purposes other than those specified at the time of collection, except with the customer's consent or as authorized by law or regulation.

4. Definitions

TEGL 39-11 provides the following definitions:

PII- 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 any specific individual.

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

Protected PII- 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 logins or passwords.

Non-Sensitive PII- Information that, if dislocated 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, e-mail addresses, business addresses, business telephone numbers, general education credentials, gender, or race. However, 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 e-mail address, or business address will most likely 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.

Federal Definitions

§200.79 Personally Identifiable Information (PII)

PII means 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. Some information that is considered to be PII is available in public sources such as telephone books, public Websites, and university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.

5. Policy

The WDB and AJC will gather information about customers/clients only through lawful means. Any subsequent use of the information is limited to purposes not inconsistent with the purpose(s) given at the time of collection. State and Federal laws state that some information submitted or accessed by customers/clients may become public records under the Public Records Act. However, there are limitations that protect this personal information from inclusion with public records. The WDB and AJC do not sell personally identifiable information.

E-mail is considered a communication tool; any data sent by customers/clients via e-mail are not secured or encrypted by the local Workforce Development Board or the American Job Centers within Union County. Customers/clients must be fully informed about the risks of electronic communication. For example, when customers fill out surveys or send the WDB or AJC e-mail messages, the e-mail address and information submitted may be collected and provided to other organizations to better serve customers' needs. However, customers shall be strongly discouraged from sending any confidential or personal data via e-mail such as social security numbers, account numbers, credit card numbers, or other data that could be compromised and compromise their privacy or identifty.

Customers are responsible for protecting the confidentiality of any user IDs, passwords, and PINs. They shall be clearly informed that if they give their user IDs, passwords, or PINs to anyone else, they are risking unwelcome access to their confidential information.

They shall be informed to contact _____immediately at ( ) ___ ____ if they believe their account is being accessed without their authorization and, if they wish to modify or update any information received by WDB or AJC, to please contact _____@.gov.

Furthermore, customers should be told in writing that, when they view information on the local workforce system's Websites, some non-confidential data may be collected, such as time and date of access and pages visited. The Website may place and subsequently, retrieve simple text files called "cookies" that identify them and their computer internet node to the workforce system's Internet site. Customer/clients shall be informed that cookies do not contain personal or confidential information about them and these will not be tracked by the staff and only be used to monitor aggregate website activity.

The Union County WDB and the American Job Center shall take appropriate steps to ensure data privacy and security by various means, including through password and user identification verification, data encryption, confidential transmissions, secure storage areas, and audit trails. Personal information shall not be sold. to any non-governmental third party. Personal information shall not distributed to any governmental third party without customers' consent or as authorized by law or regulation.

WDB and AJC employees shall only use personal information submitted by customers on a need-to-know basis and only in order to provide information or services. Personal information subitted shall not be used or stored any longer than necessary. If no longer required and in order to prevent unauthorized access or use of the data, personally identifiable information shall be destroyed via purging, magnetic degaussing/erasing, shredding and/or other means of authorized confidential destruction.

Regularly scheduled archiving, purging, and proper disposal of records and information is a standard practice throughout Union County Government Offices.

While the WDB and AJC use reasonable efforts to include accurate and up-to-date information on there Websites, content is provided by a variety of sources, changes frequently, and makes no representations or warranties as to its accuracy.

The Union County Workforce Development Board and the American Job Center understand the importance of maintaining customer privacy and shall make every attempt to maintain trust and confidence of customers and members of the community regarding the collection and use of personal information.

The policy further diictates that all customers shall receive a copy of this policy and a summary statement addressed to them affirming WDB and AJC's commitment to protecting their personal priovacy and treating their personal data with strict confidentiality.

6. Supporting Regulations

§200.337 Restrictions on public access to records.

No Federal awarding agency may place restrictions on the non-Federal entity that limit public access to the records of the non-Federal entity pertinent to a Federal award, except for protected personally identifiable information (PII) or when the Federal awarding agency can demonstrate that such records will be kept confidential and would have been exempted from disclosure pursuant to the Freedom of Information Act (5 U.S.C. 552) or controlled unclassified information pursuant to Executive Order 13556 if the records had belonged to the Federal awarding agency. The Freedom of Information Act (5 U.S.C. 552) (FOIA) does not apply to those records that remain under a non-Federal entity's control except as required under §200.315 Intangible property. Unless required by Federal, state, local, and tribal statute, non-Federal entities are not required to permit public access to their records. The non-Federal entity's records provided to a Federal agency generally will be subject to FOIA and applicable exemptions

§200.303 Internal controls.

The non-Federal entity must:

(a) Establish and maintain effective internal control over the Federal award that provides reasonable assurance that the non-Federal entity is managing the Federal award in compliance with Federal statutes, regulations, and the terms and conditions of the Federal award. These internal controls should be in compliance with guidance in "Standards for Internal Control in the Federal Government" issued by the Comptroller General of the United States or the "Internal Control-Integrated Framework," issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).

(b) Comply with Federal statutes, regulations, and the terms and conditions of the Federal awards.

(c) Evaluate and monitor the non-Federal entity's compliance with statutes, regulations and the terms and conditions of Federal awards.

(d) Take prompt action when instances of noncompliance are identified including noncompliance identified in audit findings.

(e) Take reasonable measures to safeguard protected personally identifiable information and other information the Federal awarding agency or pass-through entity designates as sensitive, or the non-Federal entity considers sensitive consistent with applicable Federal, state, local, and tribal laws regarding privacy and obligations of confidentiality.

7. Questions

For general questions regarding this guidance, contact _____at _____.gov

8. Action

This directive is to be made available to appropriate staff and incorporated within participant handbook and covered fully in participant orientation.