Handling and Protection of Personally Identifiable Information (PII)

It is the responsibility of Rivers East Local Area Staff, Program Operator Staff, NCWorks Career Center Staff and partners providing services within the NCWorks Career Centers to protect all personally identifiable information when working with customers, including employers. This includes redacting any unnecessary PII data when using for verification.

Program Operators are required to take aggressive measures to mitigate the risks associated with the collection, storage, and dissemination of sensitive data including PII. This information is generally found in personnel files, participant files, performance reports, program evaluations, grant and contract files and other sources.

Definitions

Personally Identifiable Information (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.

Sensitive Information is defined as any unclassified information whose loss, misuse, or unauthorized access to or modification of could adversely affect the interest or the conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act.

Protected PII and non-sensitive PII - the US Department of Labor 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.

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, voiceprints, iris scans, etc.), medical history, financial information and computer passwords.

2. Non-sensitive PII 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. 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 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. This demonstrates why protecting the information of our program participants is so important.

Protected PII is the most sensitive information that you may encounter in the course of your program work, and it is important that it stays protected. Operators are required to protect PII when transmitting information, and are required to protect PII and sensitive information when collecting, storing and/or disposing of information as well.

Before collecting PII or sensitive information from WIOA applicants/participants, Program Operators must have applicants/participants sign the Rivers East Personally Identification Release Form, acknowledging the use of PII for grant purposes only.

All staff must adhere to the following actions:

- Use appropriate methods for destroying sensitive PII in paper files (i.e., shredding or using a burn bag) and securely deleting sensitive electronic PII.
- Do not leave records containing PII open and unattended.
- Store documents containing PII in locked cabinets when not in use.
- **At a minimum all instances of an individual's driver's license, credit card numbers, bank account numbers, and the first five digits of the SSN must be redacted.**

All staff who will have access to sensitive/confidential/proprietary/private data must be advised of the confidential nature of the information, the safeguards required to protect the information, and that there are civil and criminal sanctions for noncompliance with such safeguards that are contained in Federal and state laws.

By signing below, I acknowledge that I have read the above referenced guidance and have received a copy of the Rivers East Local Area Issuance 2021-19 regarding the handling and protection of Personally Identifiable Information (PII), that I am aware of the safeguards required to protect the information, and that there are civil and criminal sanctions for noncompliance with such safeguards that are contained in Federal and state laws.

_____
Printed Name

_____ _____
Signature Date

_____
Affiliated Agency