STATE OF MAINE
DEPARTMENT OF LABOR
BUREAU OF EMPLOYMENT SERVICES
55 STATE HOUSE STATION
AUGUSTA, MAINE 04333-0055

Paul R. LePage
GOVERNOR

Jeanne S. Paquette
COMMISSIONER

Subject of Policy:	**Protecting Personally Identifiable Info**	**Policy No.**	**PY15-10**
To:	· Grantees & Subrecipients Local of WIOA Titles I, II, III, & IV · Local Boards · Service Providers · E & T Program Directors/Managers	**From:**	**Edward Upham, Director** **Bureau Employment Services**
Issuance Date:	**July 1, 2016**	**Status:**	**ACTIVE**
Reference/ Authority:	· TEGL 39-11 · Privacy Act of 1974 · OMB Memorandum M-06-15 *Safeguarding Personally Identifiable Information* · OMB Memorandum M-06-19 *Reporting Incidents Involving PII*		

Purpose: To provide guidance regarding requirements for Confidentiality and Handling and Protection of Personally Identifiable Information (PII).

Background: Service provider agencies involved in the administration and implementation of the Workforce Innovation and Opportunity Act (WIOA) have access to, and utilize, large quantities of personally identifiable information, including PII related to their agency/organization, their employees/staff and the individual program participants they serve. Such information is found in personnel files, participant data files, MIS tracking systems, performance reports, program evaluations, and other grant related files and data systems.

Grant recipients, subrecipients, and contractors are required to take aggressive measures to ensure confidentiality and to mitigate risks associated with the collection, storage, and dissemination of Personally Identifiable Information (PII). Safeguarding personally identifiable information and preventing its breach are essential to maintaining the public's trust.

A breach of PII can occur in many ways, including: loss of paper files, loss of control over MIS files, compromise of MIS systems, unauthorized disclosure of PII, unauthorized access to PII, and transmittal of PII via unprotected methods.

Definitions

- **Awardees** are agencies who are direct recipients, subrecipients, or subcontractors of WIOA funded programs for the purpose of this policy.

- **Confidentiality** is the act of entrusting agency or agency staff members with confidential information and adherence to rules and procedures that limit access or place restrictions on access to, use of, or sharing of, certain types of information, such as system security passcodes or personal information.

- **PII** refers to information which can be used to distinguish or trace an individual's identity, either alone or in combination with other personal or identifying information that is linked or linkable to a specific individual.

- **Sensitive Information** is any unclassified information whose loss, misuse, or unauthorized access to or modification of could adversely affect the interest of the agency program or the privacy to which individuals are entitled under the Privacy Act.

- **Protected PII and Non-Sensitive PII** the USDOL has defined two types of PII – protected and non-sensitive. The differences between protected and non-sensitive PII is based on an analysis regarding the "risk of harm" that could result from 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. For example: social security numbers (SSNs), credit card or bank account numbers, home telephone numbers, ages, birthdates, marital status, spouse names, educational history, biometric identifiers (fingerprints, voiceprints), 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, such as stand-alone information that is not linked or associated with any protected or unprotected PII. Examples include: first and last names, email addresses, business addresses, business phone 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. For example, disclosure of a person's name along with an SSN and/or date of birth could result in identity theft.

Requirement:
Awardees must implement policies and procedures that ensure that the requirements of this policy are met.

Confidentiality:
In order to maintain public confidence and trust, awardees must implement policies identifying standards of procedure regarding staff access to and use of PII maintained in paper or electronic files, to include program reviewers and auditors. The policy must require that staff sign an affirmation of their understanding of the policy and assurance that they:

1. Will not, except as necessary in the normal course of business, divulge employer, claimant, customer, participant, or co-worker information obtained in the performance of their official duties to any person within or outside of the agency unless specifically authorized to do;

2. Will not obtain information through agency computers, documents, or other official means for any purpose other than official business;

3. Will not duplicate, alter, use or disclose any information obtained through such systems or documents without proper authorization;

4. Will not, except as necessary in the normal course of business, remove documents, property or equipment containing sensitive information from the workplace under any circumstances, unless authorized to do so;

5. Will not access personal information maintained by the agency pertaining to his/her relatives, neighbors, or any other individuals that staff person is not authorized to access as part of his/her regular duties;

6. Will not disclose agency computer security codes, passwords, or combinations thereof to the public, friends, relatives or co-workers;

7. Will not trace, attempt to duplicate or otherwise forge a claimant, employer, customer, participant, vendor or co-worker signature on any document.

Access, Transmittal, Sharing, Storage and Destruction of Personally Identifiable Information
Awardees must develop and implement policies that:

- Establish levels of authority (permissions and protocols) for access to PII to ensure that access to such information is restricted only to those who require it in their official capacity.
- Ensure that PII is not transmitted to unauthorized users, by requiring that all PII and other sensitive data transmitted via email or stored on CDs, DVDs, Thumb Drives, etc. is encrypted using FIPS 140-2 compliant standards http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf**.**
- Ensure that **un**encrypted sensitive PII is not emailed to anyone.
- Ensure that PII is obtained in conformity with applicable federal and state laws governing confidentiality of information.
- Ensure and acknowledge that all PII data obtained shall be stored in an area that is physically safe from access by unauthorized persons at all times and that all data will be processed using authorized equipment or IT systems.
- Ensure that access to, processing of, and storage of PII data on any employee's personally owned equipment, home, or home computer is strictly prohibited.
- Ensure that staff members with access to PII are advised of the confidential nature of the information, the safeguards they must follow to protect that information, and the fact that there are civil and criminal sanctions for non-compliance with such safeguards contained in federal and state laws.
- Ensure that staff members acknowledge their understanding of the confidential nature of the data and the safeguards they must comply with regarding handling such data, as well as the fact that they may be liable to civil and criminal sanctions for improper disclosure.
- Ensure that all PII information will be processed in a manner that will protect the confidentiality of records/documents with safeguards in place to prevent unauthorized persons from retrieving records by unauthorized computers, remote terminals or any other means.
- Ensure that PII data requested by USDOL ETA is not disclosed to anyone but the individual requestor.
- Ensure that data downloaded to, or maintained on official mobile devices is encrypted using NIST validated software products and based on FIPS 140-2 encryption.
- Ensure that wage data may only be accessed from secure locations.
- Ensure that inspection of data for the purpose of conducting audits, reviews, or other investigations occurs only during regular business hours and that such entities abide by the confidentiality requirements described above.
- Ensure that authorized auditors, reviewers or inspectors that have been provided access to such records have such access only during the specific timeframes in which they are conducting their audit or review.

Awardees that fail to comply with these requirements, or that have improperly disclosed or utilized PII information for an unauthorized purposes are at risk of termination or suspension of their grant and imposition of special conditions or restrictions as deemed necessary to protect the privacy of the participants or the integrity of data.

Custody of PII Records:
Federal law requires that Personally Identifiable Information and other sensitive information be protected during the collection, storage and disposal processes.

Before collecting PII or sensitive information from participants or agencies with information about participants, ensure that signed releases acknowledging the use of the specific PII is only for grant purposes.

Always use a unique identifier when referencing a participant. While SSNs may initially be required for performance tracking purposes, a unique identifier must be linked to each individual record. Once the SSN is entered for performance tracking purposes the unique identifier must be used in place of the SSN for tracking purposes. SSNs must be stored or displayed in a way that is not attributable to a particular individual, such as using a truncated SSN.

Use appropriate methods for destroying sensitive PII in paper files by shredding or depositing in a secure shredding bin and securely delete sensitive electronic PII using special software designed to do so.

Never leave records containing PII open and unattended, ensure that paper records are locked away in file cabinets and ensure that your work PC locks every so many minutes and that it requires a secure passcode to unlock it.

Ensure that passcodes are complex enough that they cannot be guessed by potential hackers.

Ensure that computer passwords are secure and never share passwords with anyone (not even your supervisor or co-worker).

Breach of PII
Any breach of PII must be reported immediately to MDOL. MDOL has protocols in place to inform and protect affected participants/employees should a breach occur.

In the event of a fire or natural disaster (flood, storm, earthquake) Awardees must have a written plan in place in place pertaining to file recovery or proper file destruction.

Staff Training
Awardees must ensure that all staff receives awareness training of the requirements pertaining to confidentiality and access, handling and protection of PII; of the consequences of breach of or misuse of PII and the requirement to sign a statement acknowledging their understanding of these requirements.

Questions may be directed to:

Ginny Carroll, Division Director
MDOL BES
SHS 55, Augusta, ME 04333-0055
Phone: 207-623-7974
Virginia.A.Carroll@maine.gov