MISSISSIPPI DEPARTMENT OF EMPLOYMENT SECURITY
Policy Number 35
PERSONAL IDENTIFIABLE INFORMATION (PII)
Workforce Innovation and Opportunity Act
Office of Grant Management

1. PURPOSE AND SCOPE

Staff members who have the ability to access personal identifiable information (PII) must follow guidelines to protect said information. The information is commonly located in data sets, personnel files, reports, grant files, program evaluations, and other sources. Federal law requires that PII and other valuable information be protected at all times.

2. PARTIES AFFECTED

The following policy applies to all MDES staff members, grantees, subgrantees, and any other individuals or groups involved in the handling and protecting of PII for programs serving participants who receive WIOA, and other Department of Labor funded discretionary grants that are administered by the Office of Grant Management.

3. DEFINITIONS

a. **Personal Identifiable Information (PII)**-information that can be used to perceive or trace an individual's identity, whether it is alone or combined with other personal information which may lead to a specific individual (2 CFR 200.79).

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

c. **Protected PII**-confidential information that, if disclosed, could result in harm to the individual whose identity is linked to the information. Some examples of PII would include: credit card numbers, social security numbers, telephone numbers, bank account numbers, birth dates, age, date of birth, marital status, fingerprints, and even computer passwords.

d. **Non-sensitive PII**-information that would not cause personal harm if it happened to be disclosed. Examples of non-sensitive PII would include: first and last names, business addresses, business telephone numbers, education credentials, gender, and race.

e. **Electronic Records**-information evidencing any act, transaction, occurrence, event, or other activity stored by electronic means and capable of being accurately reproduced in forms perceptible by human sensory capabilities.

f. **Physical Records**-includes records in paper or other analog formats, such as audio tape or video tape. This does not include items that are stored in digital format on a computer, server, or a form of digital media/electronic records.

4. REQUIREMENTS

All parties must ensure the privacy of all PII obtained from participants and protect such information from unauthorized disclosure. All parties must ensure that PII used has been obtained in conformity with applicable Federal and State laws and policies governing the confidentiality of information (2 CFR 200.303 (e), TEGL 39-11).

Any PII transmitted through email or stored on external devices must be encrypted. PII that is stored on-site must be protected from unauthorized individuals at all times and must be managed with suitable services from the IT department. Storing, processing, and accessing PII data on personally-owned appliances at off-site locations is prohibited.

All individuals who may have access to confidential information and private data must be advised of the confidential status of the information, the importance of protecting the information, and that they could be liable to civil and criminal sanctions if improper disclosure is present.

It is important that PII data is processed correctly to protect the confidentiality of records and documents. This is designed to prevent unauthorized individuals from gaining access to the PII records by any means.

5. RECOMMENDATIONS

a. Prior to collecting PII from individuals, have them sign a release that acknowledges the use of PII. Similar to the attached: "Personal Information Release Form."

b. Instead of using social security numbers to identify individuals, possibly use unique identifiers to follow up with subgrantees.

c. Staff should use appropriate methods for destroying physical and electronic PII files. This would incude the act of shredding physical copies and deleting electronic files.

d. Do not leave records containing PII open and unsupervised.

e. When not in use, store PII in locked cabinets.

f. Report any suspicion of breach or breach of PII immediately.

g. REQUIRED ACTION

Local Workforce Development Boards must adopt a policy that aligns with the state policy. LWDAs will ensure that procedures align with state and local policy.

h. EFFECTIVE DATE

This policy shall be effective upon signature and will remain in effect until revised or rescinded.

R Stewart

Robin Stewart
Interim Executive Director
Mississippi Department of Employment Security

1/18/2022
Date

ATTACHMENTS

a. Personal Information Release

b. TEGL 39-11

Personal Information Release

I certify, to the best of my knowledge, that ALL information given is true. I agree and understand any willful misstatement of facts may cause forfeiture of my status in the Workforce Innovation and Opportunity Act (WIOA) program and could be cause for legal action. I understand the information is subject to verification and agree to provide such documentation as required or approval to obtain such. I understand that any information provided may be shared with other federal, state, and local or non-government agencies.

2. I authorize agencies and schools, as appropriate, to release to the WIOA Provider information necessary for verifying appropriate applicant intake responses on which program eligibility or ineligibility was based. I understand this information may subsequently be released to the grant recipient, to Workforce Development Areas and/or worksites for eligibility purposes.

3. I agree to notify the WIOA Provider of any address or phone number changes during the time I am in the program. I also understand that someone representing the WIOA provider may call me after program completion. I agree to provide them with information about my employment status, earnings, and other information necessary to evaluate program success.

4. Photo/Video Release (mark appropriate response)

   ☐ I authorize and give my permission for the WIOA Program to use quotes and take pictures/video shots of me while enrolled in the WIOA Program. These photos/videos may be used for workforce program publicity such as newspaper articles, PowerPoint presentations, website photos, etc.

   ☐ I Do Not authorize and give my permission for the WIOA Program to use quotes or take pictures and video shots of me while enrolled in the WIOA Program.

5. Data Sharing Acknowledgement
   I acknowledge that by receiving WIOA services in the state of Mississippi personal information collected during registration for and administration of these services may be disclosed to WIOA partner agencies (including, but not limited to, Mississippi Community College Board, Mississippi Department of Human Services, Mississippi Department of Employment Security, and Mississippi Department of Rehabilitation Services) or their authorized representatives to improve the quality of case management and match records to meet performance accountability, reporting, and evaluation requirements under WIOA (Pub. L.113-128). I hereby acknowledge and consent to the release of my personal information as indicated.

6. Your answer to this question is voluntary: Do you, a family member, or friend have a history of opioids or drug use? ☐ Yes ☐ No ☐ Prefer not to respond

By signing below, I hereby acknowledge and consent to the items detailed in 1-6 above.

Participant's Signature Date

Parent's/Guardian's Signature (if required) Date

By signing below, I hereby certify that the items in 1-6 above were explained to the participant and/or parent/guardian.

WIOA Provider Staff Date

EMPLOYMENT AND TRAINING ADMINISTRATION ADVISORY SYSTEM U.S. DEPARTMENT OF LABOR Washington, D.C. 20210	CLASSIFICATION Personally Identifiable Information
	CORRESPONDENCE SYMBOL OFAM
	DATE June 28, 2012

ADVISORY: TRAINING AND EMPLOYMENT GUIDANCE LETTER NO. 39-11

TO: ALL DIRECT ETA GRANT RECIPIENTS
ALL STATE WORKFORCE AGENCIES
ALL STATE WORKFORCE LIAISONS
STATE WORKFORCE ADMINISTRATORS
STATE AND LOCAL WORKFORCE INVESTMENT BOARDS
ONE-STOP CAREER CENTER SYSTEM LEADS

FROM: JANE OATES
Assistant Secretary

SUBJECT: Guidance on the Handling and Protection of Personally Identifiable Information (PII)

1. Purpose. To provide guidance to grantees on compliance with the requirements of handling and protecting PII in their grants.

2. Background. As part of their grant activities, Employment and Training Administration (ETA) grantees may have in their possession large quantities of PII relating to their organization and staff; subgrantee and partner organizations and staff; and individual program participants. This information is generally found in personnel files, participant data sets, performance reports, program evaluations, grant and contract files and other sources.

Federal agencies are required to take aggressive measures to mitigate the risks associated with the collection, storage, and dissemination of sensitive data including PII. The Appendix lists a brief overview of efforts at the Federal level to protect PII. As the grantor agency, ETA is providing this Training and Employment Guidance Letter (TEGL) to grantees to notify them of the specific requirements grantees must follow pertaining to the acquisition, handling, and transmission of PII.

3. Definitions.

- PII - OMB defines PII 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.[1]

[1] OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007), available at http://www.whitehouse.gov/OMB/memoranda/fy2007/m07-16.pdf

RESCISSIONS None	EXPIRATION DATE Continuing

- Sensitive Information – 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 Department of Labor (the Department) 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, 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, 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 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.

4. Requirements. Federal law, OMB Guidance, and Departmental and ETA polices require that PII and other sensitive information be protected. ETA has examined the ways its grantees, as stewards of Federal funds, handle PII and sensitive information and has determined that to ensure ETA compliance with Federal law and regulations, grantees must secure transmission of PII and sensitive data developed, obtained, or otherwise associated with ETA funded grants.

In addition to the requirement above, all grantees must also comply with all of the following:

- To ensure that such PII is not transmitted to unauthorized users, all PII and other sensitive data transmitted via e-mail or stored on CDs, DVDs, 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.[2] Grantees must not e-mail unencrypted sensitive PII to any entity, including ETA or contractors.

- Grantees must take the steps necessary to ensure the privacy of all PII obtained from participants and/or other individuals and to protect such information from unauthorized disclosure. Grantees must maintain such PII in accordance with the ETA standards for information security described in this TEGL and any updates to such standards provided to the grantee by ETA. Grantees who wish to obtain more information on data security should contact their Federal Project Officer.

- Grantees shall ensure that any PII used during the performance of their grant has been obtained in conformity with applicable Federal and state laws governing the confidentiality of information.

- Grantees further acknowledge that all PII data obtained through their ETA grant shall be stored in an area that is physically safe from access by unauthorized persons at all times and the data will be processed using grantee issued equipment, managed information technology (IT) services, and designated locations approved by ETA. Accessing, processing, and storing of ETA grant PII data on personally owned equipment, at off-site locations e.g., employee's home, and non-grantee managed IT services, e.g., Yahoo mail, is strictly prohibited unless approved by ETA.

- Grantee employees and other personnel 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.

- Grantees must have their policies and procedures in place under which grantee employees and other personnel, before being granted access to PII, acknowledge their understanding of the confidential nature of the data and the safeguards with which they must comply in their handling of such data as well as the fact that they may be liable to civil and criminal sanctions for improper disclosure.

- Grantees must not extract information from data supplied by ETA for any purpose not stated in the grant agreement.

- Access to any PII created by the ETA grant must be restricted to only those employees of the grant recipient who need it in their official capacity to perform duties in connection with the scope of work in the grant agreement.

[2]For more information on FIPS 140-2 standards and cryptographic modules, grantees should refer to FIPS PUB 140-2, located online at: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

- All PII data must be processed in a manner that will protect the confidentiality of the records/documents and is designed to prevent unauthorized persons from retrieving such records by computer, remote terminal or any other means. Data may be downloaded to, or maintained on, mobile or portable devices only if the data are encrypted using NIST validated software products based on FIPS 140-2 encryption. In addition, wage data may only be accessed from secure locations.

- PII data obtained by the grantee through a request from ETA must not be disclosed to anyone but the individual requestor except as permitted by the Grant Officer.

- Grantees must permit ETA to make onsite inspections during regular business hours for the purpose of conducting audits and/or conducting other investigations to assure that the grantee is complying with the confidentiality requirements described above. In accordance with this responsibility, grantees must make records applicable to this Agreement available to authorized persons for the purpose of inspection, review, and/or audit.

- Grantees must retain data received from ETA only for the period of time required to use it for assessment and other purposes, or to satisfy applicable Federal records retention requirements, if any. Thereafter, the grantee agrees that all data will be destroyed, including the degaussing of magnetic tape files and deletion of electronic data.

A grantee's failure to comply with the requirements identified in this TEGL, or any improper use or disclosure of PII for an unauthorized purpose, may result in the termination or suspension of the grant, or the imposition of special conditions or restrictions, or such other actions as the Grant Officer may deem necessary to protect the privacy of participants or the integrity of data.

5. Recommendations. Protected PII is the most sensitive information that you may encounter in the course of your grant work, and it is important that it stays protected. Grantees are required to protect PII when transmitting information, but are also required to protect PII and sensitive information when collecting, storing and/or disposing of information as well. Outlined below are some recommendations to help protect PII:

- Before collecting PII or sensitive information from participants, have participants sign releases acknowledging the use of PII for grant purposes only.

- Whenever possible, ETA recommends the use of unique identifiers for participant tracking instead of SSNs. While SSNs may initially be required for performance tracking purposes, a unique identifier could be linked to the each individual record. Once the SSN is entered for performance tracking, the unique identifier would be used in place of the SSN for tracking purposes. If SSNs are to be used for tracking purposes, they 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 (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.

- Immediately report any breach or suspected breach of PII to the FPO responsible for the grant, and to ETA Information Security at ETA.CSIRT@dol.gov, (202) 693-3444, and follow any instructions received from officials of the Department of Labor.

6. **Inquiries.** Questions should be addressed to the appropriate Regional Office.

7. **Attachment.** Appendix: *Applicable Federal Laws and Policies Related To Data Privacy, Security and Protecting Personally Identifiable and Sensitive Information*

APPENDIX

FEDERAL LAWS AND POLICIES RELATED TO DATA PRIVACY, SECURITY AND PROTECTING PERSONALLY IDENTIFIABLE AND SENSITIVE INFORMATION

- Privacy Act of 1974 (the Privacy Act) – Governs the collection, maintenance, use, and dissemination of personally identifiable information about individuals maintained in systems of records by Federal agencies. The Privacy Act prohibits the disclosure of information from a system of records without the written consent of the individual, unless the disclosure is permissible under one of twelve statutory exceptions. The Privacy Act also provides individuals with a way to seek access to and amendment of their records and establishes various agency record-keeping requirements. The Privacy Act does not generally apply to personally identifiable information collected and maintained by grantees.

- Computer Security Act of 1987 – Passed to improve the security and privacy of sensitive information in Federal computer systems and created a means for establishing minimum acceptable security practices for such systems. It required agencies to identify their computer systems that contained sensitive information, create computer security plans, and provide security training of system users or owners on the systems that house sensitive information. It was repealed by the Federal Information Security Management Act (FISMA).

- FISMA – Enacted as Title III of the E-Government Act of 2002, FISMA required each Federal agency to develop and implement an agency-wide program to safeguard the information and information systems that support the operational assets of the agency, including the assets managed by other agencies or contractors.

- On May 22, 2006, the Office of Management and Budget (OMB) issued M-06-15, *Safeguarding Personally Identifiable Information*. In this memorandum, OMB directed Senior Officials for Privacy to conduct a review of agency policies and processes and to take necessary corrective action to prevent intentional or negligent misuse of, or unauthorized access to, PII.

- On July 12, 2006, OMB issued M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*. In this memorandum, OMB provided updated guidance for reporting of security incidents involving PII.

- On May 10, 2006, Executive Order 13402 established the President's Task Force on Identity Theft. The Task Force was charged with developing a comprehensive strategic plan for steps the Federal government can take to combat identity theft and recommending actions which can be taken by the public and private sectors. On April 23, 2007, the Task Force submitted its report to the President, titled "Combating Identity Theft: A Strategic Plan." This report is available at www.idtheft.gov.

- On May 22, 2007, OMB issued M 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information. In this memorandum, OMB required agencies to implement a PII breach notification policy within 120 days.

- NIST SP 800-122, Guide to Protecting the Confidentiality of PII – Released by NIST in April 2010, this document is a guide to assist Federal agencies in protecting the confidentiality of PII in information systems. The guide explains the importance of protecting the confidentiality of PII in the context of information security and explains its relationship to privacy. The document also suggests safeguards that may offer appropriate levels of protection for PII and provides recommendations for developing response plans for incidents involving PII.