COMMONWEALTH OF PUERTO RICO

LOCAL LABOR DEVELOPMENT BOARD

SOUTHWEST LABOR DEVELOPMENT BOARD, INC.

PUBLIC POLICY REGARDING THE USE OF PERSONALLY IDENTIFIABLE INFORMATION OF CUSTOMERS AND PARTICIPANTS OF TITLE I WIOA PROGRAMS

Section 1. The Southwest Local Workforce Development Board, Inc. based on Public Law 113-128, Workforce Innovation and Opportunity Act (WIOA), creates Public Policy regarding the Use of Personally Identifiable Information of WIOA Title I Customers and Participants.

Section 2. Legal Reference

- Public Law 113-128, Opportunity and Innovation Act of July 22, 2014, Section 122 (d)(4) - "Identification of Eligible Providers of Training Services".
- Workforce Innovation and Opportunity Act (WIOA) Federal Regulations Section 603, "Federal State Unemployment Compensation (UC) Program; Confidentiality and Disclosure of State UC Information".
- "Training and Employment Guidance Letter", No. 5-08
- "Training and Employment Guidance Letter", No. 39-11

Section 3. Definition of the Term

Social Security is defined as one of the most sensitive methods of personal identification that a person can have, therefore, in order to prevent misuse, avoid identity theft and put individuals at risk, this Public Policy is created as a requirement of the Federal Law and the Employment Training Administration to protect this information of clients and participants.

Section 4. Collection of Sensitive Information

The Local Board establishes the following mechanisms to collect sensitive and identifiable information from WIOA customers and participants, such as social security. The Local Board determined that it will be used in the PRIS ("Participant Record Information System"), as your ID so that in all documents this number will be used as an Identification Number.

Section 5. Information Management

In the One Stop Center (OSC) the client's personal identification will be handled as follows:

1. The staff located in the Reception Area, which is where the client establishes the first contact with the OSC, prior to their registration the interviewer will orient them on the documents they need to complete the profile and these documents are: Social Security card and a valid photo identification (ID). At the moment of requesting these documents, the interviewer will proceed to orient the client about the purpose of showing this information and at the same time will guarantee that it will be used in a confidential manner and that the mechanisms for its protection will be provided.

   Pursuant to Section 122(d)(4) of WIOA, it states that no student may be required to provide a social security number, student number, or any other identifier without written authorization from the parent or guardian authorizing him or her to provide the information in order to be in compliance with Section 444 of the General Education Provisions Act (20 U.S.C. 1232g).

   After this, the customer's profile information will be filled out in the PRIS and the customer's ID (identification number), which is located at the top of the PRIS, will be registered.

   At the end of the PRIS registration stage, the client will have an interview with the interviewer and if the interviewer decides to use the Resource Center, the client will be guided by the staff of that area and will be responsible for registering in the PRIS the service offered and in turn, verify the profile information, which was provided by the Reception Area.

2. If the client applies for Title, I Program services, the handling of the client's personally identifiable information will be done in the following manner:

   The Interviewer will complete the Social Security Certification Form (CL-MIS-003), which will have the Social Security and Identification Number (ID). This document will be signed by the Interviewer and certified by the Case Manager. This form will be attached to the referral and Initial Assessment for this client to receive services.

The certification form will initially be in the custody of the Case Manager, who is responsible for certifying the same as previously stated and will then pass to the custody of the MIS Department Director upon completion of the process.

Section 6. Use of the Identification Number (ID)

All forms in the files for the different activities under Title I will not present the participant's social security number. Only the identification number (ID) of the profile will be used.

Section 7. File Manager

The Case Manager will be the person responsible for the file upon arrival at the Program Area and will collate all information in the participant's file prior to appointment. Documents submitted by State, Federal and Service Agencies that will be used to determine eligibility must have only the last four digits of the social security number.

Section 8. Data Execution

In the MIS Area based on WIOA Regulations for reporting performance data should be linked to social security numbers without reporting the social security number as an ID number.

Section 9. Finance Area

Following the basis of Section 603 "Federal State Unemployment Compensation (UC) Program; Confidentiality and Disclosure of State UC Information", in order to comply with the duties required by the State and Federal Agencies, the Finance Area will use the social security in order to comply with all the transactions that are required, but at the same time will establish a coordination with the MIS Department Supervisor to create controls that guarantee that it is being used solely and exclusively for these purposes.

Section 10. Approval and Validity

This Public Policy shall take effect upon adoption and shall remain in effect until amended or repealed by the Local Board.

Supporting Document: Policy Regarding the Use of Personally Identifiable Information of Participants of the Workforce Innovation and Opportunity Act (WIOA) Title I Programs of the Workforce Development Program of June 7, 2029 and form CL-MIS-003.

In San Germán, Puerto Rico, this May 1, 2024.

Roque Abad Ramírez Palermo

Southwest Local Board President

GOBIERNO DE PUERTO RICO
Departamento de Desarrollo Económico y Comercio
Programa de Desarrollo Laboral

7 de junio de 2019

Presidentes Juntas de Alcaldes, Presidentes Juntas Locales y Directores Ejecutivos de Juntas Locales de Desarrollo Laboral

Natasha Vazqueztell Cordero, JD
Directora
Programa de Desarrollo Laboral

POLÍTICAS RELATIVAS AL USO DE INFORMACIÓN IDENTIFICABLE PERSONAL DE LOS PARTICIPANTES DE LOS PROGRAMAS DEL TÍTULO I DE LA LEY DE OPORTUNIDADES Y DE INNOVACIÓN DE LA FUERZA LABORAL (WIOA, POR SUS SIGLAS EN INGLÉS)

A. INTRODUCCIÓN

La Guía Federal "*TRAINING AND EMPLOYMENT GUIDANCE LETTER* No. 39-11" publicada el 28 de junio de 2012, con el tema "*Guidance on the Handling and Protection of Personally Identifiable Information* (PII por sus siglas en inglés)", establece las directrices en cuanto a la utilización de datos clasificados como Información Identificable Personal (IIP) de los clientes (participantes y patronos) con acceso a los servicios ofrecidos por los programas bajo WIOA.

1. La IIP se define como información que pueda utilizarse para distinguir o rastrear la identidad de una persona, de manera singular o combinado con otros datos personales o de identificación. La IIP se clasifica de dos formas, la IIP Protegida y la IIP No Sensitiva. La IIP protegida se considera como información de una persona, cuya divulgación, puede resultar en daño a este o cuyo nombre o identidad está relacionada a esta información divulgada. Ejemplos de IIP protegida:

   - ✓ Número de Seguro Social (SS)
   - ✓ Números de Tarjetas de Crédito
   - ✓ Números de Cuentas de Banco
   - ✓ Números Telefónicos
   - ✓ Edad

- ✓ Fecha de Nacimiento
- ✓ Estatus Civil
- ✓ Nombre de Cónyuge
- ✓ Historial Educativo
- ✓ Identificadores biométricos
- ✓ Historial médico
- ✓ Información financiera
- ✓ Contraseñas de computadoras o cuentas electrónicas

2. El TEGL 39-11 complementa el aun aplicable guía, "TRAINING AND EMPLOYMENT GUIDANCE LETTER NO. 5-08", publicada el 13 de noviembre de 2008, que establece las directrices en cuanto al uso y solicitud del número de seguro social para los solicitantes a los programas federales de empleo y adiestramiento. Esta guía establece que los niveles estatales y locales tienen que requerirle a los solicitantes y participantes el número de seguro social previo a ofrecerle servicios, sin que ello implique que se denieguen servicios a cualquier participante que se niegue a proveer su número de seguro social.

3. No obstante, es necesario que, cuando se requiera a los solicitantes y participantes, el número de seguro social, se les explique que el propósito de esta solicitud es para solicitar datos importantes para el cálculo de resultados de indicadores de ejecución de los programas bajo WIOA, protegiendo la privacidad de la persona. El personal de los Centros de Gestión Única, así como todo aquel funcionario que trabaje con participantes, requerirá de estos que muestren su tarjeta de seguro social para corroborar que el número indicado, es realmente su número de SS. No obstante, por razones de seguridad, no podrán quedarse con copia de la tarjeta para incluirla en el expediente del participante. En todos los casos, el manejador de caso/planificador de carrera deberá certificar con su firma que el número de SS presentado, corresponde al participante. Esta directriz fue previamente publicada en carta a las JLDL el 24 de junio de 2010 (POLÍTICAS RELATIVAS AL USO DEL NÚMERO DE SEGURO SOCIAL DE LOS PARTICIPANTES DE WIA Y OTROS PROGRAMAS).

4. Conforme al TEGL 39-11, se considera una falta en el cumplimiento con los requisitos de dicha guía y la legislación federal a estos propósitos, el uso impropio y la divulgación de la IIP, para un propósito no autorizado. El TEGL 39-11 también establece que esta práctica pudiera resultar en la terminación o suspensión de los fondos o la imposición de restricciones con condiciones especiales u otra acción de parte de DOLETA, o lo que se estime necesario, para proteger la privacidad de los participantes y la integridad de los datos.

B. GUÍA DE UTILIZACIÓN DE DATOS IIP DE ACUERDO AL TEGL 39-11

1. Antes de Recopilar IIP o datos sensitivos de los participantes, hacer que estos firmen un relevo de conocimiento y uso del IIP para propósitos de los fondos utilizados.

2. Todos los datos considerados IIP, así como otra información sensitiva transmitida por correo electrónico o guardados en Discos Compactos (CDs y/o, DVDs), "*Jump Drives*", etc. tienen que ser encriptados utilizando "*Federal Information Processing Standards* (FIPS) 140-2" en cumplimiento con los "*National Institute of Standards and Technology* (NIST)[1]. El DDEC solo aceptará correos electrónicos que contengan la IIP encriptada de la forma antes descrita.

3. El TEGL 39-11 también define lo que es *IIP No Sensitivo*. Esto es información que si se divulga, no resulta en daño personal. IIP No sensitivo es información que no está relacionada o asociada de forma cercana con IIP protegido o desprotegido. Ejemplos de IIP no sensitivo es el nombre y el apellido, direcciones de correo electrónico, dirección o teléfono de negocios, credenciales educacionales, género o raza. Sin embargo, dependiendo de las circunstancias, una combinación de estos elementos potencialmente puede ser categorizado como IIP protegido o sensitivo.

4. Mientras sea posible, DOLETA recomienda el uso de los identificadores únicos para el seguimiento a los participantes, en lugar del número de SS. Mientras que el número de SS se utiliza para propósitos de ejecución, un número único de identificación puede ser enlazado a los expedientes de cada participante. Una vez el número de SS se entre en el "software" que maneja la información de participantes, para propósitos de seguimiento de ejecución, el número único de identificación debe ser utilizado en vez del número de SS. El número de SS tiene que estar almacenado o enseñado en una forma que no sea atribuible a una persona en particular.

5. Utilizar métodos apropiados para destruir IIP sensitiva de los expedientes físicos (trituración o utilizar "burn bags") y borrar de forma segura la IIP electrónica sensitiva.

6. No dejar expedientes físicos que contengan IIP, abiertos o sin atender. El custodio de los expedientes se hace responsable de salvaguardar la información contenida en estos.

7. Archivar documentos que contengan IIP en gabinetes cerrados y seguros, cuando no estén en uso.

8. Informar inmediatamente cualquier brecha o violación sospechosa del IIP al oficial federal encargado de los fondos y al "ETA Information Security" al ETA.CSIRT@dol.gov, (202) 693-3444 y seguir las instrucciones recibidas de parte los oficiales de ETA.

C. ACCIÓN A SEGUIR POR PARTE DE las Juntas Locales de Desarrollo Laboral

1. Velar por el cumplimiento de las guías TEGL 5-08 y TEGL 39-11, el marco legal WIOA, el marco legal del Programa de Seguro por Desempleo y Circular de Casa Blanca relacionada

[1] https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf

a los aspectos confidenciales y sensitivos de los expedientes en papel y electrónico, especialmente con lo relacionado la utilización del número de seguro social de los clientes.

2. Llevar a cabo una auto-validación/monitoría/auditoría de todos los expedientes de los participantes y hacer los cambios necesarios para demuestrar el cumplimiento con el marco legal referido. El resultado de este ejercicio es corroborar que el número de seguro social no esté visible en ningún formulario o documento de apoyo dentro del expediente físico del participante. Reiteramos que este ejercicio no implica, que no se solicitará/obtendrá el número de seguro social de la persona (Ver Sección A.3., B.I. y B.3.). Este debe estar en el expediente electrónico del participante de forma protegida, siguiendo los parámetros antes mencionados.

Para mayor información respecto a las políticas del uso de IIP, se incluyen copias de las guías TEGL 5-08, 39-11 y carta a las JLDL del 24 de junio de 2010. Esperamos y contamos con su acostumbrada atención en el cumplimiento de estas directrices.

De necesitar asistencia técnica o de tener dudas con esta información, favor comunicarse con la señora Yolanda Rivera Ortiz, Directora del Área de Planificación, Evaluación, Validación y Estadísticas del Programa de Desarrollo Laboral, al (787)754-5504, extensión 5618/5619 o al correo electrónico yolanda.rivera@ddec.pr.gov .

24 de junio de 2010

PRESIDENTES DE JUNTAS DE ALCALDES, PRESIDENTES DE JUNTAS LOCALES Y DIRECTORES EJECUTIVOS ÁREAS LOCALES DE INVERSIÓN EN LA FUERZA TRABAJADORA

Aurelio González Cubero
Director Ejecutivo

POLÍTICAS RELATIVAS AL USO DEL NÚMERO DE SEGURO SOCIAL DE LOS PARTICIPANTES DE WIA Y OTROS PROGRAMAS

La Carta Núm. 5-08 titulada "Training and Employment Guidance Letter (TEGL), emitida el 13 de noviembre de 2008, establece las directrices en cuanto al uso y solicitud del número de Seguro Social (SS) para los potenciales participantes con acceso actividades bajo WIA y a otros servicios de programas de la fuerza trabajadora.

La reglamentación aplicable establece que los estados tienen que requerirles a los participantes su número de SS cuando estén ofreciendo los siguientes servicios, **sin que ello implique que el estado pueda denegarle acceso a cualquier participante que se niegue a proveer su número de seguro social:**

- Servicios Básicos relacionados a la determinación de elegibilidad, actividades de búsqueda de empleo;
- Servicios de Adiestramiento y Empleo;
- Auto servicio.

No obstante, es necesario que, cuando se les requiera a los participantes el número de SS, los estados tienen que explicarles con qué propósito este número será utilizado e informarles sobre la manera en que se garantizará su privacidad. Estableciendo además, que los estados deben utilizar el número de seguro social sólo para propósitos de calcular los resultados de las medidas de ejecución de un programa.

Las áreas locales WIA requerirán a los participantes que muestren su tarjeta de seguro social para corroborar que el número indicado por el participante es realmente su número de SS. No obstante, por razones de seguridad, las áreas locales no podrán quedarse con copia de la tarjeta para incluirla en el expediente del participante. En todos los casos, el manejador de caso deberá certificar con su firma que el número de SS presentado corresponde al participante.

Es importante reiterar que el estado no puede denegarle acceso a cualquier participante que se niegue a proveer su número de seguro social.

Para mayor información respecto a las políticas del uso del SS, se incluye copia del TEGL Núm. 5-08. Esperamos y contamos con su acostumbrada atención especial en el cumplimiento de estas directrices.

De necesitar información adicional sobre el particular, puede comunicarse a nuestra Oficina de Asuntos Legales a las extensiones 300 ó 306.

Anejo

EMPLOYMENT AND TRAINING ADMINISTRATION ADVISORY SYSTEM U.S. DEPARTMENT OF LABOR Washington, D.C. 20210	CLASSIFICATION WIA/Performance Measures
	CORRESPONDENCE SYMBOL PROTECH
	DATE November 13, 2008

TRAINING AND EMPLOYMENT GUIDANCE LETTER NO. 5-08

TO: ALL STATE WORKFORCE LIAISONS
ALL STATE WORKFORCE AGENCIES

FROM: Brent R. Orrell
Deputy Assistant Secretary

SUBJECT: Policy for Collection and Use of Workforce System Participants' Social Security Numbers

1. Purpose. To provide guidance to states regarding the collection and use of social security numbers for participants accessing Workforce Investment Act (WIA) and other workforce programs' services.

2. References. Privacy Act of 1974, 5 U.S.C. section 552a Note; Workforce Investment Act of 1998, 29 U.S.C. section 2935; Performance Accountability under Title I of the Workforce Investment Act, 20 CFR 666.150; Income and Eligibility Verification System, 20 CFR 603; Training and Employment Guidance Letter (TEGL) 17-05, *Common Measures Policy for the Employment and Training Administration's (ETA) Performance Accountability System and Related Performance Issues.*

3. Background. States face a difficult challenge of balancing the need to collect a participant's social security number for performance and reporting requirements with the obligations to limit the burden of data collection and maintain participant privacy. To that end, this guidance provides clarification about the point at which a state should request a participant's social security number for WIA and other workforce system purposes.

   ETA's statutory and regulatory authority to administer job training and employment programs includes provisions requiring performance reporting from states and other grantees on participant outcomes. ETA has provided guidance to states that a program participant is an individual who is determined eligible to participate in the program and receives a service funded by the

RESCISSIONS	EXPIRATION DATE Continuing

program in either a physical location or remotely through electronic technologies. (TEGL 17-05, Section 6 (Program Participation and Exit under Common Measures)). Consistent with that guidance, program participation begins on the first date that the individual receives a service funded by the program. Program participation also marks the point at which all participants, except some self-service participants, become part of the pool of participants used to calculate performance measure outcomes.

States are required, consistent with state law, to use quarterly wage record information in measuring the progress against state and local performance measures. (20 CFR 666.150) States must use social security numbers to match a program participant's records with that individual's quarterly wage record information to assess the impact of program services.

4. Policy. When requesting a participant's social security number, states should explain how the social security number will be used and how a participant's privacy will be ensured. For purposes of compliance with ETA training programs, states must use social security numbers only for the calculation of program performance measure outcomes. States must ensure that social security numbers will be maintained in a secure and confidential manner. State workforce agencies are responsible for following the requirements pertaining to the confidentiality and disclosure of state unemployment compensation information (which includes wage records) found at 20 CFR 603.

ETA interprets WIA to permit the prohibition of disclosure of a participant's social security number. This prohibition springs from WIA section 185(a)(4). WIA section 185(a)(4) states that records maintained by states must be made available to the public upon request with certain exceptions. These exceptions include the disclosure of information that would constitute a clearly unwarranted invasion of personal privacy and privileged or confidential financial information. (WIA section 185(a)(4)(B)) A participant's social security number is entitled to this exception.

This guidance does not imply or require that a participant provide a social security number to the state to receive services through WIA or any other workforce investment program, with the exception of a participant filing a claim for unemployment compensation. In instances where a participant does not provide a social security number, states should exclude the outcomes of this individual from performance measures, unless supplemental information is available to verify the performance outcomes for non-wage based measures, which is consistent with established policy.

Section 7 of the Privacy Act (5 U.S.C. Section 552a Note (Disclosure of Social Security Number)) provides that unless the disclosure is required by Federal statute, "It shall be unlawful for any Federal, state or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number." Again, the one exception is that claimants filing for unemployment insurance must provide their social security number.

5. Guidelines. The following are guidelines for states regarding when to request a participant's social security number. States should not consider these guidelines exhaustive. States may collect a social security number at an earlier point of service; however, such decisions must be defined by official state policies and shared with the appropriate One-Stop staff. States must request a participant's social security number when offering the following services, keeping in mind that the state must not deny access to any participant who refuses to provide a social security number:

   - Staff-Assisted Core Services related to eligibility determination, job search activities, and employment. These services would include activities such as: staff-assisted career guidance including the development of an employability and/or individual employment plan, assessments, career guidance and counseling, customized labor market information, resume assistance, federal bonding assistance, job search assistance, job referrals, and career workshops.

   - All Training and Education Services. These services include assessment tests used to ascertain a participant's educational level and/or employability, occupational skills training, on-the-job training, educational and job training counseling, referrals to educational services, and pre-vocational training and related services.

   - Self-Services. These services are those that an individual accesses independently without staff assistance, either in a physical One-Stop Center, or remotely via the Internet. States should be clear that a social security number will be requested if and when a person who accesses self-services requests any staff-assisted service and/or is seeking to access more intensive services. Visitors who wish to review the list of services available through a One-Stop Center, who want to access labor market information, or who are conducting a job search without the assistance of staff and do not request a referral to a specific job may take advantage of self-service activities offered through the state's One-Stop Centers without providing a social security number.

In addition to the services listed above, social security numbers shall be requested when a participant is co-enrolling in a program that offers intensive training services or provides financial assistance (for example, a Trade Adjustment Assistance Relocation Allowance).

6. Inquiries. States may contact the appropriate Regional Office if they have any questions or need further clarification on this guidance.

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	EXPIRATION DATE
None	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*

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.

CL-MIS 003 Rev. Enero 2023

CONEXIÓN LABORAL
ÁREA LOCAL SUROESTE

AmericanJobCenter
Área Suroeste

Plaza Pitito Carr. # 2 Km. 170.0 Bo. Hoconuco P.O. Box 246 San Germán, Puerto Rico 00683
Tel. (787) 787-892-1000 Fax (787) 892-5540 TTY (787)-892-2935 Libre de Cargos 1-800-981-8155

CERTIFICACIÓN DE SEGURO SOCIAL

Yo, _____, certifico que verifiqué la tarjeta de Seguro Social con el

número ☐☐☐■☐☐■☐☐☐☐ correspondiente al solicitante _____.

Hoy _____ de _____ de _____. Número de Identificación (ID _____.

Comentarios:

_____

_____

_____

_____

_____ _____
Nombre del Representante Autorizado/CL/AJC Firma del Representante Autorizado/CL/AJC

_____ _____
Nombre del Manejador de Casos o Representante Autorizado Firma del Manejador de Casos o Representante Autorizado

_____ _____
Puesto del Representante Autorizado Fecha

Nota: *Favor de entregar formulario junto con la Hoja de Control de Nombramiento al Departamento de MIS.*

Somos un Patrono con Igualdad de Oportunidad en el Empleo. Contamos con Servicios Auxiliares y de Apoyo para Personas con Impedimento que así lo soliciten. El CL/AJC No Discrimina por Razón de Raza, Color, Religión, Sexo, Nacionalidad, Edad, Impedimento Físico o Mental, Afiliación o Creencia Política. El CL/AJC es un Centro Libre de Drogas y Alcohol. Ley Federal "Workforce Innovation and Opportunity Act/WIOA". Financiado con el 100% de los Fondos de la Ley de Innovación y Oportunidades en la Fuerza Laboral (WIOA). Ley Pública 113-128 del 22 de julio de 2014.