COMMONWEALTH OF VIRGINIA
VIRGINIA COMMUNITY COLLEGE SYSTEM

**WORKFORCE INVESTMENT ACT**

**VIRGINIA WORKFORCE LETTER (VWL) #14-02**

| | |
|---|---|
| **TO:** | LOCAL WORKFORCE INVESTMENT BOARDS |
| **FROM:** | WORKFORCE DEVELOPMENT SERVICES |
| **SUBJECT:** | Guidance on the Handling and Protection of Personally Identifiable Information (PII) |
| **DATE:** | December 1, 2014 |

---

**REFERENCES:**

Training and Employment Guidance Letter No. 39-11; Subject: *Guidance on the Handling and Protection of Personally Identifiable Information (PII);* Dated June 28, 2012

**Purpose:**

To provide guidance to Local Workforce Investment Areas (LWIAs) and their service providers on compliance with the requirements of handling and protecting Personally Identifiable Information (PII) in their programs.

**Background:**

As a result of a recent compliance review by staff from the Region 2 office of the U.S. Department of Labor Employment and Training Administration, there was a finding that requires the development of a policy to address Personally Identifiable Information (PII).

As part of their grant activities, Local Workforce Investment Areas 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.

The guidance is provided to LWIAs to notify them of the specific requirements they must follow pertaining to the acquisition, handling and transmission of PII.

**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.

**Sensitive Information** – any classified 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 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.

> *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 Number (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.
>
> *Non-sensitive PII*, on the other hand, is information that if disclosed, by it, could not reasonably be expected to result in personal harm. Essentially, it is stand-alone information that is not likely 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.

**Requirements:** Federal law, OMB Guidance, and Employment and Training Administration 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 the transmission of PII and sensitive data developed, obtained or otherwise associated with ETA funded grants.

In addition to the requirement above, all Local Workforce Investment Areas (LWIAs) and Virginia Community College System (VCCS) programs funded with Workforce Investment Act (WIA) resources 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 email or stored on CDs, DVDs, thumb drives, etc., must be encrypted. Any participant information should not include: Social Security Numbers (SSNs) or Date of Birth (DOB). Information concerning a participant should include only: State ID, User Name or User ID from the Virginia Workforce Connection (VaWC) when provided as part of a data correction or related VaWC transaction. If the question is related to performance and/or reporting, the State ID, User ID or User Name should be the only identifier used in communications with appropriate VCCS staff. Grantees/sub-grantees must not email sensitive PII to an entity, including ETA or contractors.

- LWIAs and VCCS programs supported by WIA funds 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. LWIAs and VCCS programs supported by WIA funds must maintain such PII in accordance with the ETA standards for information security described in TEGL 39-11 and any updates to such standards provided to the ETA grantee (VCCS). Staff from a LWIA or VCCS program supported by WIA funds should contact VCCS for additional information on data security.
- LWIAs and VCCS programs funded by WIA funds shall ensue that 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.
- LWIAs and VCCS programs funded by WIA funds 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/subgrantee 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 and/or VCCS.
- LWIAs and VCCS programs funded by WIA funds 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 law.
- LWIAs and VCCS programs funded by WIA funds must have their policies and procedures in place under which administrative and program employees, 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.
- LWIAs and VCCS programs funded by WIA funds must not extract information from WIA (ETA) funded programs for any purpose not stated in the grant agreement, contract, and/or memorandum of understanding (MOU).
- Access to any PII created by the ETA grant must be restricted to only those employees of the grant recipient, LWIAs and VCCS programs funded by WIA funds that need it in their official capacity to perform duties in connection with the scope of work in the grant agreement, contract of MOU.
- 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 and properly secured. Wage data may only be accessed from secure locations and access to wage information may be limited based on agreements between VCCS and other entities (Virginia Employment Commission [VEC], Wage Record Interchange System [WRIS and WRIS 2], and Federal Employment Data Exchange [FEDES]).
- PII data obtained through a request from ETA must not be disclose 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 (to include: LWIAs and VCCS programs funded by WIA funds) is complying with the

confidentiality requirements described in the Virginia Workforce Letter. In accordance with this responsibility, granted (to include: LWIAs and VCCS programs funded by WIA funds) must make records available to this Agreement (to include: grant agreement, contract of MOU) available to authorized persons for the purpose of inspection, review and/or audit.

- Grantees (to include: LWIAs and VCCS programs funded by WIA funds) 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 (to include: LWIAs and VCCS programs funded by WIA funds) agree to destroy the data using appropriate processes related to the data (for example: deletion of electronic data).

A grantee's (to include: LWIAs and VCCS programs funded by WIA funds) failure to comply with the requirements included in this VWL (and TEGL 39-11), or any improper use or disclosure of PII for an unauthorized purpose, may result in the termination or suspension of the grant, contract or memorandum of understanding, or the imposition of special conditions or restrictions, or such as the Grant Officer may deem necessary to protect the privacy of participants or the integrity of data.

**Recommendations:** Protected PII is the most sensitive information that you may encounter in the course of your work, and it is important that it stays protected. All organizations receiving WIA funds 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. The following recommendations may help in protecting PII.

- Before collecting PII or sensitive information from participants, have the participants sign releases acknowledging the use of PII for grant purposes only.
- Whenever possible, ETA and VCCS recommend 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 each individual record. VaWC uses the State ID, which is a system-generated number not related to the SSN. Once the SSN is entered for performance tracking, the unique identifier would be used in place if 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 Workforce Development Systems office of the Virginia Community College System.
- Do not use any PII as identifiers on participant file folders.