COMMONWEALTH OF VIRGINIA
VIRGINIA COMMUNITY COLLEGE SYSTEM

WORKFORCE INNOVATION AND OPPORTUNITY ACT

The Virginia Community College System
VIRGINIA WORKFORCE LETTER (VWL) No. 19-05

TO:	Local Workforce Development Boards
FROM:	George Taratsas Director, WIOA Administration
SUBJECT:	Guidance on the Handling and Protection of Personally Identifiable Information (PII)
EFFECTIVE DATE:	October 24, 2019

PURPOSE:
To provide guidance on compliance with the requirements of handling and protecting Personally Identifiable Information (PII) in WIOA Title I programs.

REFERENCES:
Training and Employment Guidance Letter No. 39-11; Subject: *Guidance on the Handling and Protection of Personally Identifiable Information (PII)*; Date June 28, 2012
2 CFR §200.79 Personally Identifiable Information
2 CFR §200.82 Protected Personally Identifiable Information
Code of Virginia §2.2-3803. Administration of system including personal information; Internet privacy policy; exceptions
Code of Virginia §18.2-186.6. Breach of Personal information notification

REVISION HISTORY:
This guidance replaces VWL # 14-02, Guidance on the Handling and Protection of Personally Identifiable Information (PII), dated December 1, 2014.

DEFINITIONS:

Personally Identifiable Information (PII) – the Office of Management and Budget (OMB) has defined 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 conduct of Federal programs, or the privacy to which individuals are entitled to 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 of 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 itself, 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.

Wi-Fi – a facility allowing computers, smartphones, or other devices to connect to the Internet or communicate with one another wirelessly within a particular area.

BACKGROUND:

As part of their grant activities, Local Workforce Development Boards and WIOA Title I service providers handle applicant and participant data that includes PII. The protection and security of this information is critical to ensure no harm is done to the applicant/participant.

GUIDANCE:

Federal law, Office of Management and Budget (OMB) directives, DOL Employment and Training Administration (ETA) policies, and the *Code of Virginia* 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 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, any program or entity that receives WIOA Title I funding must 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 transmitted participant information should not include Social Security Numbers (SSNs) or Date of Birth (DOB). Transmitted information concerning a participant should include only State ID, User Name or User ID from the Virginia Workforce Connection (VaWC) or last name only when provided as part of a data correction or related VaWC transaction. If the action 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. Grantee/subgrantees must not provide sensitive PII to an entity, including ETA or contractors.
- All programs supported by WIOA Title I funds must take the steps necessary to ensure the privacy of all PII obtained from participants and other individuals and to protect such information from unauthorized disclosure. These programs 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 (WIOA Title I Administrator). Staff from a program supported by WIOA Title I funds should contact the WIOA Title I Administrator for additional information on data security.
- Programs funded by WIOA Title I 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.
- Programs funded by WIOA Title I are required to ensure 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, and managed information technology (IT) services. 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 prohibited. It is highly recommended that a Virtual Private Network (VPN) is utilized when accessing PII in an offsite location. The WIOA Title I Administrator urges all users to be mindful of how and where they are accessing PII where it may be compromised such as over public/unsecured wifi networks or where documents containing PII may be observed by the general public.
- For programs funded by WIOA Title I, employees and other personnel who will have access to sensitive/confidential/proprietary/private data must be advised in writing 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.
- Programs funded by WIOA Title I must have their policies and procedures written and in place under which administrative and program employees, before being granted access to PII, shall acknowledge in writing their understanding of the confidential nature of the data, the safeguards with which they must comply in their handling of such data, and understand they may be liable to civil and criminal sanctions for improper disclosure.

- Programs financially supported by WIOA Title I must not extract information from WIOA (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 and programs funded by WIOA Title I that need it in their official capacity to perform duties in connection with the scope of work in the grant agreement, contract, or 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 written agreements between the WIOA Title I Administrator (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 disclosed to anyone but the individual requestor, except as permitted by the Grant Officer.
- Grantees (programs funded by WIOA Title I) must permit ETA and Auditor of Public Accounts 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 in this Virginia Workforce Letter.
- Grantees (to include: programs funded by WIOA Title I) must retain data only for the period of time required to use it for assessment and other service provision related purposes consistent with applicable state and federal records retention requirements. Upon completion of the grant activities, the grantee agrees to destroy the data using appropriate processes related to the data (for example: deletion of electronic data).
- Programs funded by WIOA should not access VaWC using public Wi-Fi unless they are using a VPN because of the potential for data breaches.

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, such as the grant administrator 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 WIOA Title I 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 actions must be taken help in protecting PII.

- Before collecting PII or sensitive information from participants, have the participants sign releases acknowledging the use of PII for the provision of services only.
- Whenever possible, ETA and the WIOA Title I Administrator 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 (such as xxx-xxx-x513)

- Use appropriate methods for destroying sensitive PII in paper files (e.g.., shredding or using a burn bag) and securely deleting sensitive electronic PII.
- Do not leave records containing PII open and unattended.
- Documents containing PII must be in locked cabinets when not in use.
- Immediately report any breach or suspected breach of PII to the WIOA Title I Administrator.
- Do not use any PII as identifiers on participant file folders.

Data Breach

In the event that a local workforce development board or contracted service provider suspects, discovers, or is notified of a data security incident or potential breach of security relating to personal information, the LWDB shall as soon as possible, but no later than twenty-four (24) hours from the incident, notify the WIOA Title I Administrator and Grant Recipient.The WIOA Title I Administrator will notify the DOLETA Federal Project Officer assigned to Virginia about data security incident or potential breach. It is also recommended that timely notice of a breach is provided to local workforce development board members and chief local elected officials.

The notification shall include the following:

- Approximate date of the incident;
- description of cause of the security event and how it was discovered;
- number of individuals affected and the type of PII involved;
- steps taken/to be taken to remedy the event.

The LWDB or contracted service provider shall also comply with notification requirements outlined in §18.2-186.6. of the *Code of Virginia*.

INQUIRIES:

WIOA Title I Administrator
Academic and Workforce Programs
Virginia Community College System
Arboretum III
300 Arboretum Place, Suite 200
Richmond, VA 23236
Telephone: (804) 819-5387
Fax: (804) 786-8430
Email: wioa@vccs.edu