Workforce Innovation and Opportunity Act (WIOA) Administrative Policy #104

Subject: **Confidentiality and Protection of Personally Identifiable Information (PII)**

Effective Date: **July 1, 2015*; Revised November 12, 2020***

References: **USDOL Training and Employment Guidance Letter 39-11**
Virginia Workforce Letter #19-05

Policy Statement:

The Capital Region Workforce Development Board (WDB) is committed to ensuring that its WIOA Title I service providers protect the Personally Identifiable Information (PII) and other confidential information as may be obtained and recorded in the course of determining WIOA eligibility and in providing services, to include follow up.

Definitions:
PII- OMB defines PII as information that can be used to distinguish or trace an individual's identity, either along or when combined with other personal or identifying information that is linked or linkable to a specific individual.

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

1. Protected PII is defined by the US Department of Labor as that which, if disclosed, could result in harm to the individual whose name or identity is linked to that information. Examples include social security numbers, credit card numbers, bank account numbers, home telephone numbers, ages, birthdate, marital status, spouse names, educational history, biometric identifiers (fingerprints, voiceprints, iris scans etc.), medical information, financial information and computer passwords.

2. Non-sensitive PII, on the other hand, is information that if discloses, by itself, could not reasonably be expected to result in personal harm. Essentially, it is stand-alone information that tis not linked or closely associated with any protected or unprotected PII. Examples of non-sensitive PII include information such as first and last names, email addresses, business addresses, business telephone numbers, general education credentials, gender, or race. However, depending on the circumstance, 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.

The following steps shall be taken by any service provider or staff working on behalf of the WDB.

1. <u>Prior to collection of PII or sensitive personal information:</u>

    a. Individuals shall be notified that such information will only be used for purposes of service under the WIOA-funded grant program and its attendant regulations and as part of the WIOA program application sign a release acknowledging such.
    b. Individuals shall also be notified that with written consent, such information may be shared with other Virginia Workforce Network partner organizations for purposes of referral and potential coordination of services beyond WIOA.
    c. The individual may agree in writing to release all or portions of their information and be provided the opportunity to indicate what information may and may not be shared. The individual may also indicate if there are specific organization(s) to which their information may not be shared. The consent may be modified or revoked by the individual at any time by providing written notice. Customer initials should be obtained to document customer designations and subsequent changes.
    d. Unless modified or revoked by the individual, written consent shall remain in effect 4 years from the date of the last signature.
    e. WIOA-paid staff and unpaid volunteers and other personnel who will have access to sensitive/confidential/proprietary/private data must be advised by the service provider management of the confidential nature of information, the safeguards required to protect the information as described in Section 2 of this policy below and the safeguards in handling such information. Written acknowledgements from staff and other partner personnel shall be kept by the WIOA service provider(s).

2. Safeguarding of PII and sensitive information once obtained:
    a. PII of WIOA participants shall not be transmitted by email or stored on CDs, DVDs, thumb drives, etc. unless it can be encrypted using federally approved standards. Only the WDB may grant such permission, with advance written approval, at the time of the request will convey the necessary standards to be followed.
    b. In no case should PII be mailed or otherwise transmitted in hard-copy format.

c. All PII data of WIOA participants shall be stored in an area that is physically safe from access by unauthorized persons at all times and the data will be processed electronically using the state WIOA system of record as communicated. (Currently the Virtual One Stop, or VOS, that is part of the Commonwealth's Virginia Workforce Connection). Other secure systems with encryption capabilities may also be authorized by the WDB. Accessing, processing and storing of WIOA grant PII data on personally owned equipment, at off-site locations and non-grantee managed IT services is strictly prohibited unless approved by the Commonwealth of Virginia.
d. PII and sensitive data will only be retained for the retention period has defined by the Department of Labor, the Commmonwelath of Virginia and/or the WDB, and then destroyed.
e. No PII or sensitive information will be used for any purpose other than necessary under the WIA. Any information collected for customer service or continuous improvement efforts will be aggregated, reported anonymously without any connection to an individual.
f. No third-party market opinion surveys, research, panel or focus groups shall be granted access to PII and other sensitive WIOA participant information without prior written consent of the WDB.

In the event of a suspected or confirmed data breach, the local board shall notify the WIOA Title I Administrator and Grant Recipient at Virginia Community College System within 24 hours of the incident. Notice shall include the elements required in VWL 19-05 and TEGL 39-11. In addition, the individuals potentially impacted by the breach either by the Board or contracted service provider responsible for the incident will be crossed referenced with VA Code Section 18.2 – 186.6 for determination of notification and in consultation with the Henrico County Attorney's office. (Local grant recipient to the Board).

By: Brian Davis, Executive Director