Policy Memorandum 2020-11

Privacy and Data Security – Effective February 1, 2020

INTENDED AUDIENCE:	All members of the Anne Arundel County Local Workforce Development Board, board members and staff of Anne Arundel Workforce Development Corporation (AAWDC), and partner staff at the Anne Arundel County Career Center
SUBJECT:	Staff Responsibility Related to Privacy and the Protection of Personally Identifiable Information (PII) and other sensitive information
LAST REVIEWED/UPDATED:	November 2019
RESPONSIBLE OFFICE:	Office of Compliance
POLICY CONTACT:	Compliance Manager

******

CANCELLATIONS

PPM 2017-10 – Personally Identifiable Information

STANDARD OPERATING PROCEDURES

None

FORMS

None

Approvals

President and CEO, AAWDC Kirkland J. Murray (Apr 4, 2020)

Chair, Local Workforce Development Board H. Walter Townshend (Apr 4, 2020)

Introduction

The Anne Arundel County Local Workforce Development Board (Local Board) recognizes that partners within the workforce development system handle a vast amount of information about our customers and clients. Release of this information (intentional or otherwise) can be damaging if disclosed to the wrong individual or misused by staff. Personally Identifiable Information (PII) is collected on current and prospective registrants and participants, past participants, employees, Board members, etc. Additionally, partners may also collect PII on youth participants that requires additional consideration and special handling. In general, PII is protected by the following laws:

- Privacy Act of 1974
- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (FTC Information Safeguarding Rule)
- Health Insurance Portability and Accountability Act (HIPAA)
- Children's Online Privacy Protection Act
- Maryland Confidentiality of Information Act
- Maryland Social Security Number Privacy Act
- Maryland Personal Information Protection Act

Policy Statement

AAWDC shall follow all federal, state, and local requirements to protect PII and sensitive information about an individual (including jobseekers, participants in AAWDC initiatives, business customers, and employees). While the goal of this policy is to prevent a security breach, AAWDC shall promptly respond to a breach (whether real or perceived) and act to contain and minimize loss as a result of the breach to the extent practicable and as required by law.

General

The Local Board oversees Anne Arundel County's workforce development system. Partners in the system collect participant-level demographic data as required by the programs the partners administer. This data collection allows the partners to:

- Determine eligibility for participation in various program and benefits administered by the partners
- Determine eligibility for inclusion on state or local eligible training provider lists
- Determine barriers to employment and provide supportive services, where applicable
- Track and ensure that programs are assisting clients and customers as they are supposed to do
- Track outcome and performance metrics
- Track program co-enrollment
- Track any follow-up requirements with clients and customers
- Collect demographic data on various population characteristics (such as disability and homelessness)
- Assist the Local Board in understanding the local workforce development system
- Assist the partners in applying for and obtaining grants

This data is collected in a variety of means, both in electronic and physical formats.

Data Access

Per Maryland Policy Issuance 2019-04, partner agencies are required to execute Data Sharing Memorandums of Understanding (MOUs), listing the specific data elements the agency can access and what purpose the data will be used for. There are four steps to gain data access:

1. *Information Release Form* – The agency must have the participant sign an Information Release Form. The form will acknowledge that the participant understands that certain data will be shared between partner agencies to support the participant's success in gaining meaningful employment.
2. *Data Sharing MOU* – The agency must have a data sharing agreement with the Local Board and its Administrative and Fiscal entity, AAWDC.

3. *Clear Understanding of Staff Responsibilities* – The agency must have a privacy and data security policy in place which clearly defines staff confidentiality and provides a Standard Operating Procedure for gaining access to confidential information and for restricting or deactivating staff access.
4. *Staff Training* – All staff with access to a data collection system must receive training from the parent agency within 30 days of being granted access. Additionally, the agency must provide annual training on privacy and data security.

Data Security

AAWDC, on behalf of the Local Board, has established the following standards for data security.

Physical file data must be protected by the following means:

- Reduce the volume of collected physical data to the minimum necessary to fulfill the reporting requirements of the data element or case management service.
- Access to physical file data is limited to staff who require access to perform necessary job functions (called "need to know" access).
- Files must be physically stored in a central location that can be secured.
- From employment records, equal opportunity and medical data should be stored separately from employee personnel file (see 29 CFR Part 38.41 for more information).
- For participant records, medical data should be stored separately from the participant's master file.
- Files should be secured (i.e., put away in a locking drawer) before leaving for an extended period.
- Due diligence monitoring of subgrantees and vendors should be conducted on a regular schedule.
- Files should be labeled utilizing a unique identifier (such as MWE State ID) that is not protected PII.
- Files should be disposed of through confidential recycling.

Electronic file data must be protected by the following means:

- Access to electronic records should be limited to staff who require access to perform necessary job functions. Access should be restricted to read only where a staff's necessary job functions does not require data entry or data validation job functions.
- Electronic files should utilize encryption and strong authentication procedures to make information unusable to unauthorized users.
- Data containing Protected PII should not be transmitted through electronic means, such as e-mail, unless encrypted (whenever possible) and shall not be transmitted through temporary memory devices (such as USB drives).
- Logging out of electronic data collections systems, such as MWE, when leaving the computer unattended.
- Use of aggregated data whenever possible.

Records Retention

Agencies must typically retain participant files and corresponding electronic data for a period of three years after the grant closeout date. For formula grants, the guideline is three years after participant's exit cohort close date. Fiscal data must be retained for seven years after the grant closeout date. These are de minimum standards. If an agency has requirements that differ from these standards, it is incumbent upon staff to be aware of those standards.

Definitions

Exit Cohort – An exit cohort is all exiters between July 1st and June 30th of a Program or Fiscal Year. The close date is July 1 of the next program year.

Personally Identifiable Information (PII) is any information pertaining to an individual that can be used to distinguish or trace a person's identity, on its own or in combination with other information that is linkable to that individual.

PII comes in many forms as indicated in the table below:

Type of Data	Definition	Examples
Protected PII	Information that, if disclosed, could result in harm to the individual whose identity is linked to that information.	• Social Security Numbers • Credit card numbers • Home telephone numbers • Age and/or birth date • Marital status and/or spouse name • Educational history • Biometric identifiers (i.e., fingerprints) • Medical history • Financial information • Computer passwords
Non-sensitive PII	Information that, if disclosed, by itself, could not reasonably be expected to result in personal harm. It is stand-alone information that is not linked or closely associated with any protected or unprotected PII.	• First and last names • E-mail addresses • Business addresses and/or phone numbers • General education credentials • Gender • Race

Record is the original or any copy of a document, regardless of form or medium, that is created, received, and maintained by AAWDC in pursuance of its legal obligations or in the transaction of business.

Related Policies and Other Resources

- Federal, state, or local policies
  - *TEGL 39-11* – Guidance on the Handling and Protection of Personally Identifiable Information (PII), dated June 28, 2012
  - *TEGL 07-16* – Data Matching to Facilitate WIOA Performance Reporting, dated August 23, 2016
  - *TEGL 05-08* – Policy for Collection and Use of Workforce System Participants' Social Security Numbers, dated November 13, 2008
  - *Office of Management and Budget Memorandum 07-16* – Safeguarding Against and Responding to the Breach of Personally Identifiable Information, date May 22, 2007
  - *Policy Issuance 2019-04* – Privacy and Data Security, dated March 28, 2019
  - *AAWDC Policy Memorandum 2020-04* – Incident Reporting, dated October 1, 2019
  - *AAWDC Privacy and Data Security Essentials Training*

Revision History

Policy Number	Date of Revision	Significant Change
2017-10 – Personally Identifiable Information	1/1/2017	Initial Policy