ANNE ARUNDEL
WORKFORCE DEVELOPMENT
CORPORATION

Policy and Procedure Memorandum 2017-WDB- 10

Personally Identifiable Information (PII) – Effective January 1, 2017

TO: Anne Arundel Workforce Development Corporation (AAWDC) staff
Subgrantees
Vendors

FROM: Kirkland Murray
President and CEO
Anne Arundel Workforce Development Corporation

SUBJECT: Protection of Personally Identifiable Information (PII)

PURPOSE: To ensure that any staff who collects or uses PII complies with the appropriate state and federal regulations and exercises due diligence and care for information security.

ACTIONS: Directors will ensure that all employees are educated on and have received copies of this policy. All AAWDC PPMs shall be posted on the Shared drive.

EXPIRATION: N/A

QUESTIONS: Jason W. Papanikolas, MBA
Policy and Compliance Analyst
410-424-3250
jpapanikolas@aawdc.org

******

CANCELLATIONS

None

AAWDC Approvals

MWC Office of Research, Performance and Compliance
— Fiscal Office
— Program Director
KJM President and CEO
HMF Workforce Development Board

General Information

As a workforce entity, AAWDC, the Anne Arundel County Career Centers, and our state and local partners handle a vast amount of information about our customers and clients that can damaging if disclosed to the wrong individual or misused by staff. Personally Identifiable Information (PII) is any information pertaining to an individual that can be used to distinguish or a trace a person's identity, on its own or in combination with other information that is linkable to an individual. PII is collected on current and prospective registrants and participants, past participants, employees, Board members, etc. Prospective and current participants in AAWDC youth programs also require additional consideration and special handling. Due to the nature of its work, AAWDC, Career Center staff, and our partners may have access to PII that is protected by more than federal, state, and local law. In general, PII is protected by the following laws:

- 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 Medical Records Act
- Maryland Social Security Number Privacy Act
- Maryland Personal Information Protection Act

The table below provides examples of different types of PII. Please note that list is not exhaustive and is not intended to cover every possible example.

Examples of PII that may require legal notification of breach	Examples of Other Protected PII that is considered Sensitive/Confidential	Examples of Other PII with the potential for misuse
Social Security Numbers	Educational records	Date of birth
Driver's license numbers	Grades, transcripts, schedules	User credentials (MWE State ID)
Financial account information	Personal financial information (not including account information)	Last 4 of SSN
Credit card number	Employment records	Student ID numbers

The following information is considered to be Public PII. This means that the information is available in public sources, such as telephone books, public websites, etc. While the information on its own is not protected by privacy laws and regulation, the information may be combined together or other protected PII and may produce a privacy breach.

- First and last name
- Address
- Work telephone number
- Work e-mail address
- Home telephone number
- General educational credentials
- Photos and videos

PII Protection Policy

AAWDC, the Anne Arundel County Career Centers, and our partners may collect PII in paper, electronic records, and in oral communications, as well as aggregated in an electronic format (i.e. databases, spreadsheets, tables, Sharepoint). When PII is collected, the following considerations must be made:

1. In general, AAWDC requires that all legal requirements be followed in the collection, use, disclosure, transmission, storage, and disposal of PII.
2. Appropriate safeguards must exist to protect against inappropriate access, use, disclosure, or transmission of PII. These safeguards include, but are not limited to, storing paper records in a secured location, keeping laptops secured when away from a desk (i.e. signed out of MWE), and encrypting data prior to transmission via e-mail. The Office of Research, Performance and Compliance will monitor initiatives, subgrantees, and vendors to ensure that appropriate safeguards are in place.

3. Collection of PII should be conducted in such a way as to minimize the potential for exposure. Collected PII should be appropriate for the intended purpose. PII should not be aggregated, unless necessary and then only for the business purpose needed.
4. Access to PII is based on the principle of "need to know." Individuals accessing PII must be permitted to do so by law or regulation and must have a legitimate "need to know" the information. The authorization to access PII is specific to that need. In other words, an intake specialist may need to know an individual's date of birth in order to determine program eligibility and can access the information that enables the specialist to know that specific information.
5. Disclosure to third party may only occur as required law or regulation. AAWDC has established that access to PII is limited to such information as may be needed to fulfill the request. At all times, PII collected by AAWDC shall remain in AAWDC's control or the control of its subgrantees. Participant data is not subject to Freedom of Information Act, but may be subject to the Maryland Public Information Act. AAWDC staff and subgrantees should direct all information requests to the Office of Research, Performance and Compliance.
6. PII should not be collected orally in a public space. AAWDC cannot ensure that such PII will not be overheard by individuals not authorized to access it. If PII must be collected orally, staff are advised to collect such information in a private area where the opportunities for accidental transmission can be minimized.
7. Disposal of information must be conducted according to the relevant law or regulation. In general, AAWDC follows 20 CFR 97.42 to guide decision-making on information retention. This regulation specifies that information must be retained for at least three years after the Program Year in which a customer exits (for formula grants) or at least three years after the Program Year in which the program ends (for discretionary grants).
8. All staff should be trained on PII disclosure and must sign a confidentiality agreement. Additional confidentiality agreements may be needed to access certain records (such as MWE or unemployment insurance data. Confidentiality agreements should be on file with Human Resources and/or the local MIS administration as necessary.

It is the responsibility of the AAWDC Executive and Leadership Teams to ensure that these guidelines are followed by all employees, contractors, vendors, and volunteers.

Reporting and Monitoring

Any breaches, real or potential, must be reported immediately to the Office of Research, Performance and Compliance (RCP). Examples of data breach include misplacing a participant file, loss of a laptop, mobile device, or removable media (i.e. flash drive), accidental e-mail of PII, virus or malware attack on a computer containing PII.

The RCP Office will conduct a thorough investigation of the breach to include:

- Extent and nature of breach
- What data was accessed (or potentially accessed)
- What safeguards were in place to prevent breach and were these safeguards followed

Participants will be notified by AAWDC that there PII was potentially breached within 10 days of AAWDC discovering the breach. AAWDC will offer additional safeguards to participants as required by law.

Employees who are found to be in violation of this policy may be subject to disciplinary action as deemed appropriate based on the facts and circumstances of the violation.