Data Security and Protection of Personally Identifiable Information (PII)

In accordance with TEGL 39-11, the definition of PII as defined by the Office of Management and Budget (OMB) is 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 link or linkable to a specific individual.

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 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 numbers (SSNs), credit card numbers, bank account numbers, Driver's License numbers, telephone numbers, ages, birthdates, marital status, spouse names, educational history, biometric identifiers (fingerprints, voiceprints, iris scans, etc.), medical history, financial information and computer passwords.

2. 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 linked 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 program participants is so important.

Staff Roles & Responsibilities:

To maintain customer and employee data protection, all staff with access to participant-level data must:

- Complete the Staff Confidentiality Agreement for Access to MD DOL's MWE/VOS User Data every six months and submit it to the Director, Office of Workforce Development:
- Maintain client confidentiality and protect PII, sensitive information, confidential UI data, and educational records;
- Inform DLLR of any users who were previously granted access to a MD DOL data system and need to be restricted or inactivated within ten business days of decision to inactivate user;
- Participate in training for the protection of PII and sensitive information on-hire and on an annual basis; and
- Notify mandated and relevant parties in the case of a security breach, as outlined on pages 13-15 of Policy 2019-14, and as required by other legal or contractual requirements.

Board approved 9/22/2023

Data Training Responsibilities:

Any staff with access to electronic or physical participant-level data must undergo training on the handling and protection of data as well as protocol in case of a breach (1) upon hire and (2) annually afterwards.

Protection of Data and Sensitive Information

Physical Data Security Requirements:

Physical data refers to paper files, as required for record retention, auditing, and often used in case management. Safeguards to protect physical data must include:

・ Reducing the volume of collected and retained physical data to the minimum necessary as is needed for reporting, eligibility determination, and case management;

・Limiting access to those individuals who must have access to perform job functions;

・Keeping files in cabinets and offices that lock;

・Keeping equal opportunity data (e.g. medical information and requests for accommodations) in files separate from employees' personnel files in accordance with 29 CFR Part 38.41;

・Ensuring that all cabinets and offices are locked before leaving the office unattended;

・Ensuring that files are not left out (e.g. on a desk during a lunch break) where an unauthorized individual can access them;

・Developing and adopting a risk-aware culture;

・Conducting due diligence on all third-party service providers and requiring appropriate information security standards to be written into contracts;

・Developing and testing an incident response plan, which should involve key stakeholders:

・Using unique identifiers to de-identify records and remove PII (e.g. new unique number specific to organization versus use of social security number);

・Using locked boxes when transferring data for auditing; and

・Using confidential recycling to dispose of records.

Retention and Disposal of Physical Records:

Local and state partners must maintain participant-level data for specific timeframes according to the type of record, including three years for workforce program data, seven years for fiscal data, or until all audit and litigation issues are resolved, whichever is later. If any litigation, claim, or audit is started before the expiration of the standard retention period, the records then must be retained until all litigation, claims, or audit findings involving the records have been resolved and final action has been taken.

Once the mandated amount of time has passed for a physical record, and the record is not needed as follow-up to an audit finding or concern, then the record may be disposed of. Disposal must take the form of confidential recycling, such as with a cross-cut shredder or through a vendor.

Electronic Data Security Requirements:

Electronic data refers to participant-level data retained in electronic data systems, such as the MWE.
These data banks contain large sources of data that are necessary for state and program function but are also potential vulnerable targets for breaches. Safeguards to protect electronic data must include:

・Reducing the volume of collected and retained electronic data to the minimum necessary;

・Limiting data access to only those individuals who must have such access;

・Using password-protection, encryption-preferred, strong authentication procedures, and other security controls to make the information unusable by unauthorized individuals (necessary when transmitting PII through email or other electronic format; e.g. staff may not email social security numbers without encryption, even if the email is addressed to an individual that has authorized access);

・Immediately deleting received emails containing unencrypted PII and instructing the sender to also delete (including removing from the "deleted files" folder) the email from their "sent" and "deleted files" folders;

・Ensuring that data is not left unattended (e.g. MWE data must not be left open on screen while on a lunch break);

・Logging out of data systems when leaving one's desk;

・Limiting network access to approved devices certified with appropriate security controls;

・Not accessing data systems from non-secure computers (e.g. personal computer);

・Conducting due diligence on all third-party service providers and requiring appropriate information security standards to be written into contracts;

・Following all electronic and physical record requirements when scanning a document into a data system, including not using PII or sensitive information in the naming convention of scanned documents;

・Developing and testing an incident response plan, which should involve key stakeholders; and

・When receiving data requests:

- Providing aggregate-level data (i.e. all PII and sensitive information removed and performance numbers combined to represent the whole program or class) or
- If participant-level is required, only providing participant-level data if the entity or partner has an MOU in place.

Retention and Disposal of Electronic Records:

Participant-level data must be maintained for specific timeframes according to type of record. The retention periods of electronic files should match the physical file schedules for corresponding records. After the retention period has passed, electronic records should be cleared, purged, or destroyed, such that the PII and sensitive information cannot be retrieved. The receipt of electronic records from other entities may be subject to additional requirements defined by specific data sharing agreements.

Security Breaches

The term "breach" is used to indicate the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic. Breaches can be the result of a spontaneous incident (e.g. data system error), security incident (e.g. break-in), privacy incident (e.g. failure to maintain confidentiality), staff error, data breach, etc. Breaches are

hazardous both to customers and to organizations involved. Individual harm may include identity theft, embarrassment, or blackmail. Organizational harm may include a loss of public trust or legal liability.
Upon discovery of a security breach, organizations are required to notify affected parties and oversight agencies, assess the level of potential harm as a result of the breach, develop a Corrective Action Plan, and activate the incident response plan

Recognizing A Security Breach Has Occurred

Security breaches vary by cause, magnitude, and effect. Thus, there are multiple ways to recognize that a security breach has occurred. If a staff member suspects that a security breach has occurred, they must notify their supervisor immediately in order to investigate whether there has been an incident. Examples of warning signs that a security breach has occurred include:

- Missing files or documents,
- Signs of a break-in or attempted break-in to office or cabinets,
- Critical electronic file change,
- Unusually slow internet or devices,
- Obvious device tampering,
- Locked user accounts,
- Unusual electronic outbound traffic,
- Abnormal administrative user activity,
- Fake antivirus messages,
- Redirected internet browsing, and/or
- Unexpected software installs.

Notification To DWDAL

Breaches are subject to notification requirements, both for physical and electronic data. Upon suspicion that a breach has occurred, the individual that discovered the possible breach must immediately notify their supervisor. In the event of a breach the Local Area Director (or designee), MD DOL DWDAL Director of Workforce Development, MD DOL DWDAL Manger of Monitoring and Compliance, MD DOL DWDAL Director of Office of Workforce Information and Performance, where applicable, and Affected customers/employees, and Governor's Workforce Development Board need to be notified within 3 business days. For each breach, the MD DOL DWDAL Monitoring and Compliance Manager must be notified as soon as possible. Entities must not wait to notify MD DOL until after an investigation has been conducted, for timing is essential to resolving breach issues and protecting customers and employees. The MD DOL DWDAL Monitoring and Compliance Manager, then, is in charge of notifying appropriate state and federal partners of the breach within 24 hours if the breach is assessed to have a high level of harm (high impact breach). The MD DOL DWDAL Director of the Office of Workforce Information and Performance must be notified of any electronic breach that involves the MWE.

The notifications should be brief and contain the following elements:

- A brief description of what happened, including the date(s) and rough time estimate(s) of the breach and of its discovery;
- To the extent possible, a description of the types of PII and/or sensitive information involved in the breach (e.g., full name, social security number, date of birth, home address, account number, disability code, etc.);
- What the agency, organization, or entity is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches;
- Contact information for the organization's person of contact leading the efforts for the investigation; and
- For notifications to the affected customers and/or employees, the steps that affected individuals and/or employees should take to protect themselves from potential harm.