Wednesday Webinars

Personally Identifiable Information (PII)

Chuck Dooley

January 4, 2017

Requirements

- U.S. Department of Labor
  - Training and Employment Guidance Letter No. 39-11
- Illinois State Laws
  - Identity Protection Act (5 ILCS 179)
  - Personal Information Protection Act (815 ILCS 530)
- WIOA Final Rule at 20 CFR 683.220 – Recipients and Subrecipients of WIOA title I funds must have an internal control structure and written policies in place to protect PII and sensitive information.

Requirements, Cont'd.

- Federal Uniform Guidance
  - 2 CFR 200.303(e) – Must take reasonable measures to safeguard protected personally identifiable information and other information the Federal awarding agency or the non-Federal entity designates as sensitive
- Your Employer's/Pass-Through Entity's Policies and Procedures
  - TEGL 39-11 requires that DOL ETA grantees must have policies and procedures in place under which personnel, before being granted access to PII, acknowledge their responsibilities for safeguarding data.

Definition

- DOL definition of PII
  - PII 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 linked or linkable to a specific individual. Note: There is a similar definition of PII in the Uniform Guidance at 2 CFR 200.79.

Types of PII

- Protected PII
  - Information that if disclosed could result in harm to the individual. According to the Uniform Guidance at 2 CFR 200.82, this does not include PII that is required by law to be disclosed.
- Non-Sensitive PII
  - Information that if disclosed, by itself, could not reasonably be expected to result in personal harm.

Examples of Types of PII

- Protected PII:

  social security numbers, credit card numbers, home telephone numbers, and birthdates.
- Non-Sensitive PII:

  first and last names, business addresses, and business telephone numbers.

Note: Non-sensitive PII linked to protected PII (name linked to a social security number) could result in harm to an individual.

DOL Requirements – TEGL 39-11

- PII and other sensitive information must be protected.
- Don't email sensitive PII unless it is encrypted.
- Don't store sensitive PII on portable drives or media unless it is encrypted.
- Don't access or store PII data on personally owned equipment at off-site locations.
- Access to any PII created by the ETA grant must be restricted to only those employees who need it in their official capacity to perform duties in connection with the scope of work in the grant agreement.

DOL Requirements – TEGL 39-11, Cont'd.

- If SSNs are used, they must be stored or displayed in a way that is not attributable to a particular individual.
- PII data must be stored in an area that is physically safe from access by unauthorized personnel.
- PII may not be downloaded to, or maintained on, mobile or portable devices unless it is encrypted. In addition, wage data may only be accessed from secure locations.

Common Sense Measures

- Mask PII on documents before emailing.
- Do not leave records containing PII unattended on your desk.
- Don't leave PII at the copier/printer or fax machine.
- Don't put PII in the trash. Use shredders or locked recycling bins.
- Store records with PII in secured cabinets/areas.

Common Sense Measures, Cont'd.

- Return participant files to their proper area or keep in a secure place (i.e., locked file cabinet).
- Redact PII before making copies or upload/storing documents with sensitive information.
- Do not write the password to your laptop on your laptop.

Data Security Measures

- Do not share user name and password.
- Do not share access to system accounts (GRS, IWDS, JobLink, Illinois workNet, IBIS, IES, etc.).
- Do not link unauthorized hardware to state network (example: hooking up a wireless router to state LAN line).
- Notify Network Administrator when employees are separated or suspended.

Data Security Measures, Cont'd.

- Only use system accounts for authorized business purposes.
- Do not download and install programs or software from the internet.
- Do not open suspicious emails or solicitous emails.
- Always lock your workstation when away from your desk.
- Do not store PII on zip drives, CDs, etc.

Penalties

- According to TEGL 39-11, there are civil and criminal sanctions for noncompliance with safeguards contained in Federal and state laws.
- Employees may be subject to disciplinary action, up to an including discharge, from their employers.