Indiana Department of Workforce Development | Indiana Adult Education

Personally Identified Information (PII) – Procedures to Protect Student Information
Remote Data Collection | Guidelines to Assist Indiana Adult Education Programs

Indiana Adult Education program staff are increasingly required to collect sensitive participant information when working remotely. Participant information, such as learner registration forms and assessment results, are retained and transmitted. Below are protocols to protect student information.

Adult education sub recipients must have in place policies and procedures which personnel, before being granted access to PII and other sensitive information, acknowledge their understanding of the confidential nature of the information and the safeguards with which they must comply in its handling, as well as liability to civil and criminal sanctions for improper disclosure;

- Before collecting PII from participants, have the participant sign release forms acknowledging its use, disclosing the entities that will have access to it, and notifying them that in certain circumstances the proper, secure release of their information will be necessary.
    - Use digital, or eSignature applications such as DocuSign and Adobe E-signature
    - Whenever possible use **Unique Identifiers**, such as **Participant ID or Local Assigned Number**, for participant tracking, instead of SSNs.
    - If PII needs to be stored on a shared network folder (such as a Google file), create a limited access subfolder, and provide access privileges only to those who have a need to access the information
- PII and other sensitive information is stored in a manner that protects the confidentiality of the records and documents and is designed to prevent unauthorized individuals from retrieving such records
- If data are downloaded to, or maintained on, mobile or portable devices, the data are encrypted using InTERS
- PII and other sensitive information is never left in plain sight and unattended;
- PII and other sensitive information obtained through a request is not disclosed to anyone other than an individual or entity authorized by law to receive the information. Individuals authorized by law include, but are not limited to: ➢ program staff with a need to know; ➢ auditors; ➢ state and fiscal monitors; and ➢ individuals or entities identified in a signed release from the participant.

Protection Against & Response to Possible Breaches of PII

If staff members suspect or know policy has been violated, regardless of the reason or severity, staff must;

- At the time of discovery, secure the PII from further compromise;
- Report the incident to the Supervisor or (if unavailable or there is a potential conflict of interest) to the Director;
- Notify DWD immediately of all PII breaches. Do not compromise the information further by including PII in the incident report;
- Document or maintain records relevant to the incident, as they might be required in the privacy incident handling report;
- If the incident was not a breach but PII protection policies were violated, take corrective action to minimize future incidents.

Updated: April 2020