

## **ATTACHMENT B**

### **INFORMATION TO BE ADDRESSED WHEN RELEASING PERSONALLY IDENTIFIABLE INFORMATION THROUGH THE P20 SLDS**

The following list contains information the P20 SLDS Task Force members are recommending be included in an MOU between entities sharing personally identifiable information (PII).

#### **Written Agreements Using the FERPA Audit or Evaluation Exception**

The audit or evaluation exception allows for the disclosure of PII without consent to authorized representatives of the FERPA-permitted entities (i.e., State or local educational authorities). PII must be used to audit or evaluate a Federal- or State-supported education program, or to enforce or comply with Federal legal requirements that relate to those education programs (audit, evaluation, or enforcement or compliance activity).

1. **Designate an authorized representative of a FERPA-permitted entity;**
2. **Describe the activity to make clear that it falls within the audit or evaluation exception.**
3. **Specify what PII will be disclosed and for what purpose.**
  - a. **Under the audit or evaluation exception, the purpose of data sharing can only be to carry out an audit or evaluation of Federal- or State-supported education programs, or to enforce or to comply with Federal legal requirements that relate to those programs.**
4. **Require an authorized representative to destroy PII upon completion of the audit or evaluation and specify the time period in which the information must be destroyed.**
  - a. Set terms for data destruction
    - i. Duration of agreement and timeline of data destruction upon completion of research
    - ii. Ongoing research should have a termination date and new agreement reauthorized every 48 months as an example
  - b. Specify modification and termination procedures, including approved destruction methods for each specific type of media (e.g., data wiping, degaussing, shredding, etc.)

5. **Establish policies and procedures, consistent with FERPA and other Federal, State, and local confidentiality and privacy laws, to protect PII from further disclosure and unauthorized use.**
  - a. Clearly document inherited obligations based on limitations on the source data (for example, FERPA details and obligations with Education data, etc.) occurs
6. Clearly identify PII owner and authoritative source of data
7. Agree on limitations on use of the PII, including any methodological restrictions, such as linking to other data sets
  - a. Include statutory limitations
  - b. Clearly document intended data elements to be linked to and the purpose of that link.
  - c. Document authority to link to the described data elements.
    - i. This is likely only the MOU's from the related agencies.
8. Document the authority to enter into agreement- particularly when there is an upstream owner of data.
  - a. This should include MOU's by reference and attachment
  - b. Example: WDE as custodian of district data vs. district data ownership and how they come to agreement on data redisclosure
9. Specify points of contact and data custodians
  - a. Periodic updates/continuous collaboration on the progress of working being completed in the MOU.
10. Identify penalties for inappropriate disclosure
11. Include funding terms - may be unique for individual studies
12. Maintain the right to audit
  - a. If an entity is providing data, they maintain the right to examine and inspect the premises of the entity conducting the audit or evaluation.
13. Identify and comply with all applicable legal requirements, including maintaining the data in a secure manner by applying appropriate technical, physical, and administrative safeguards to properly protect the PII, both at rest and in transit
  - a. Reference plans that are in accordance with any applicable State and Federal laws for

responding to a data breach, including, when appropriate or required, responsibilities and procedures for notification and mitigation

- b. Notification process and disciplinary steps if data breach or agreement breach
14. Review and provide feedback on reported results
    - a. Review of draft outcomes/reports by all agreed upon data owners/authoritative sources prior to release of report (*for example, if DWS links to Vital Records data at WDH under an MOU with Health while generating an Education report, Health would get to review the report prior to release*)
    - b. The data custodians will provide the upstream data owners with the opportunity to review and provide feedback on reported results.
  15. Define responsibilities and commitment to ensure agency heads are aware of data agreements in place when change occurs at agency
    - a. Responsibility of data steward to inform school districts on how the information is being used
    - b. Community college system will have a data governance system to support this
  16. Document method of re-engagement between parties if the desired use of the data exceeds that which is specifically agreed upon in MOU