IOWA'S STATE LONGITUDINAL DATA SYSTEM

SLDS Record-Level Data Request Application

See the Protocol for Requesting SLDS Data for more information.

1. **Project title:**

2. **Date of data request:**

3. **Anticipated start date for this project:**

4. **Proposed end date for the project:**

5. **SLDS partners from which merged data are required:**
   - ☐Iowa P-12
   - ☐Iowa Community Colleges
   - ☐Iowa Public Universities (Regent universities)
   - ☐Iowa Workforce Development
   - ☐Iowa College Aid

6. **Project Coordinator contact information**
   Name:
   Mailing address:
   Phone number:
   Email address:

7. Key Personnel

Name	Specific Duties on Project	Date of Human Subjects Training[1]

8. Purpose of data request:

☐ Research
☐ Program evaluation

9. Is IRB approval required?

☐ Yes *(If yes, attach IRB application or approval)*
☐ No

10. What are the objectives of this project?

11. Who will benefit from this project?

12. What other work/experience/research has already been done on this topic and is providing a framework or guide for this study (i.e., theoretical framework)?

13. What questions are you trying to answer with these data (i.e., research questions and hypotheses)?

14. Data Sample/Population

15. List of Variables Needed for the Research

16. Data Analysis/Statistical Methodology

[1] Human Subjects Training ensures that project personnel understand issues related to data on individuals. Training is available at no cost through the National Institute of Health: http://phrp.nihtraining.com/users/login.php.

17. Data security plan

Project Coordinator: initial by each of these items to signify agreement with the terms.

Initial Strong passwords and multi-factor authentication are used to restrict access to devices on which data are stored.

Initial Devices on which data are stored will automatically shut down, logout, or lock (e.g., password-protected screen saver) after 10 minutes of inactivity.

Initial Current and regularly updated anti-virus/malware software is installed on devices with access to data.

Initial Internet firewalls are turned on for devices on which data are stored.

Initial Any paper copies of record level data are secured in a locked filing cabinet.

Initial All devices on which the data are stored (e.g., laptops, tablets, flash drives, smartphones) are encrypted or stored within encrypted file folders on those devices. The physical protection of portable devices containing encrypted data is the responsibility of all key personnel.

Initial Lost or stolen devices that contain data will be reported to the SLDS team immediately.

Initial Data requestors and/or their organization must have policies in place to oversee compliance, inventory, and auditing of external devices.

Initial Cloud-hosted environments that will be used to store data are FedRAMP and/or StateRAMP authorized.

Initial Destruction of electronic data will be done by overwriting the stored data. Overwriting replaces new data in storage locations, making the previous data unreadable.

18. Where will the data be stored?

19. Dissemination and Outreach