



Minnesota Data Access & Management Policy

Approved by SLEDS Governance - October 23, 2014

Amended - November 10, 2016

Contents

- Section 1 - Overview 3
 - 1.1 Purpose 3
 - Policy Statement 3
 - 1.2 Guiding Principles 4
 - 1.3 SLEDS Contact Information 5
 - 1.4 General Information 6
 - SLEDS Data 6
 - Definitions 8
 - Maintaining the Privacy (Security) of Individual Information 11
 - Levels of Access 12
 - Unauthorized Access 15
 - Rights of Subjects of Data to Inspect and Review Data and Records 15
 - Legislation Governing Data Sharing and Data Privacy 16
 - Destruction of Data 18
- Section 2 - Procedure for Requesting Access to SLEDS 19
 - 2.1 Types of Requests 19
 - 2.2 SLEDS Data Access Request Information 20
 - Roles and responsibilities 21
 - Guidelines for Conducting SLEDS Research 21
 - Sensitive Data Elements 22
 - Qualifying FERPA Exception 22
 - 2.3 SLEDS Data Access Request Requirements 23
 - Step 1: Submit a Complete Data Access Request 23
 - Step 2: Review by coordinators 24
 - Step 3: Review by the SLEDS Research Committee 25
 - Step 4: Final Approval Process 25
 - Step 5: Completion of Research 26
- Section 3 - Policy Authorization 28
- Appendix A: Documents and Forms 29
- Appendix B: Data Matrix 48

Section 1 - Overview

Minnesota's Statewide Longitudinal Education Data System (SLEDS) brings together education and workforce data from the Departments of Education and Employment and Economic Development, and the Office of Higher Education to:

- Identify the most viable pathways for individuals in achieving successful outcomes in education and work,
- Inform decisions to support and improve education and workforce policy and practice, and
- Assist in creating a more seamless education and workforce system for all Minnesotans.

SLEDS will bridge existing education and workforce data. Using the 4P's — Pathways, Progress, Predictors and Performance, stakeholders will have a framework to assess and evaluate data from all systems in order to answer critical and long-ranging questions, while building a comprehensive body of information that can be used to inform future decision making.

1.1 Purpose

The purpose of this document is to support and promote greater understanding and use of SLEDS data. This policy provides a framework for SLEDS partners to properly manage data access in compliance with data security and other applicable policies, and state and federal law. The policy provides for transparency in data access and use.

Policy Statement

Access to SLEDS data will be as broad as possible, but will be governed by the following federal and state laws and resultant policies and procedures;

Minnesota Government Data Practices Act (MGDPA, Minn. Stat. § 13)

Family Education Rights and Privacy Act (FERPA, 34 CFR Part 99)

Confidentiality and Disclosure of Unemployment Compensation Data (CFR 20. Part 603)

See Section 1.4 for additional information about these statutes.

Additional factors that are considered when determining the level of access are:

Classification of data,

Role and responsibility of the user, and

Compliance of users with data security policies and training.

1.2 Guiding Principles

Based on the work of the SLEDS Research and Data Advisory Committee, seven guiding principles for data access and management have been established:

1. SLEDS will focus on providing cross-sector, linked data and analysis.

This principle asserts that SLEDS focuses on cross-sector data use and refers any data requests limited to just one sector (K-12 education, postsecondary education or employment) to the appropriate agency or partner data provider.

2. SLEDS relies on transparency and clarity in all we do.

Education and workforce data, including its use, will be presented in plain and readily comprehensible language and formats. SLEDS partners will maintain a level of detail and disaggregation in accordance with state and federal regulations. SLEDS policies and procedures, including roles and responsibilities of all parties, will be defined and available for all to see.

3. Protecting the privacy of individuals is a priority.

This principle governs all we do and recognizes that an individual's privacy is a primary concern for contributing state agencies, partner data providers, and users of the SLEDS system. This requires users be aware of and respect the differing data privacy requirements of the various data sets included in SLEDS.

4. Common understanding and use of data increases its value.

This principle recognizes that only common understanding and use of data allows SLEDS to empower and inform decision making. This level of understanding requires contributing state agencies and partner data providers to jointly develop an understanding of and common language regarding the transitions between systems in addition to local programs. This process requires that state agencies and partner data providers discuss and commit to overcoming the obstacles to shared understanding and use of data, including but not limited to the issues of turf, trust, technology and time.

5. Data providers, at the state and local levels, are critical sources for understanding and explaining the data.

This principle recognizes that state agencies and partner data providers are critical sources for understanding and explaining data in SLEDS. Training and opportunities for data users to connect with data providers is imperative for success. Data users should be specific and transparent in describing their methodologies and assumptions and are encouraged to vet those methods and assumptions with contributing state agencies and partner data providers.

6. Maintenance of SLEDS and the provision of research and analysis is the responsibility of all data providers.

This principle recognizes that maintenance and use of SLEDS requires the coordinated and collaborative efforts of the contributing state agencies, the Minnesota P-20 Education Partnership and partner data providers.

7. Local partner data provider access is needed for data to drive continuous improvement in local and state level policy.

This principle recognizes that access to and use of data at the local level (i.e., colleges, K-12 schools and districts, workforce programs) is valued and better informs local improvement and state policy.

1.3 SLEDS Contact Information

Questions, requests for information, data access requests, and other SLEDS-related correspondence can be directed to any SLEDS Coordinators.

Meredith Fergus

Policy Analyst / SLEDS Coordinator
Minnesota Office of Higher Education (OHE)
Meredith.Fergus@state.mn.us
651-259-3963
<http://ohe.state.mn.us>

Alex Hermida

Research Analyst / SLEDS Coordinator
Minnesota Office of Higher Education (OHE)
Alex.Hermida@state.mn.us
651-259-3919
<http://ohe.state.mn.us>

Anita Larson

Data Analytics Supervisor / SLEDS Coordinator
Minnesota Department of Education (MDE)
Anita.Larson@state.mn.us
651-582-8361
<http://education.state.mn.us/>

Rachel Vilsack

Agency Performance Manager / SLEDS Coordinator
Minnesota Department of Employment and Economic Development (DEED)
Rachel.Vilsack@state.mn.us

651-259-7403

<http://mn.gov/deed/>

- SLEDS website: <http://sleds.mn.gov>
- Minnesota P-20 Education Partnership website: <http://mnp20.org>

1.4 General Information

SLEDS Data

SLEDS includes the following data:

K-12 Enrollment: Enrollment data aggregated at the school, district, county and state levels collected from Minnesota public and private K-12 institutions, including, but not limited to, enrollment by ethnicity, gender, grade and special populations. This data is managed by MDE.

K-12 Assessment: Results from statewide assessments such as Minnesota Comprehensive Assessment-Modified (MOD), Minnesota Test of Academic Skills (MTAS), Minnesota Comprehensive Assessment (MCA) and ACCESS for English Learners. Aggregated at the school, district, county and state levels, this data includes counts and percentages of students performing at four achievement levels. This data is managed by MDE.

ACT Assessments (Explore, Plan, and College Entrance assessments): ACT's Explore, Plan, and College Entrance assessment's results for Minnesota high school students in graduating classes from 2008 to 2012 aggregated at the district and high school level. These data were provided by ACT, and reflect only the most recent test results for students who tested on more than one occasion, and may include tests taken in grades 10, 11 or 12. This data is managed by MDE.

Adult Basic Education: Adult Basic Education serves students who are 16 years old or older, not enrolled in or not eligible to attend K-12 public or private school and lack basic skills in one or more of the following areas: reading, writing, speaking, listening and mathematics. Services provided include basic skills instruction, English for Speakers of Other Languages, General Educational Development (GED) preparation, adult diploma, work readiness, family literacy and transition to postsecondary education/training. This data is managed by MDE.

Advanced Placement (AP) Results: Advanced placement exam results are scores ranging from 1 to 5 and indicate the high school student's achievement level in the specified subject area. The scores are generally used by colleges to determine if the student will be granted college credit for completion of the AP course. This data is managed by MDE.

Kindergarten Readiness: Kindergarten Readiness Assessment data is information across developmental domains for a representative sample of public school kindergartners across the state within the first several weeks of school. Data is collected by the child's teacher. This data is managed by MDE.

Early Childhood Enrollment: Early childhood enrollment includes children, birth to kindergarten, who: 1) either have an Individualized Education Plan (IEP), Individual Family Service Plan (IFSP), Individual Interagency Intervention Plan (IIIP) or received assessment for special education or 2) are pre-kindergarten students who are classified as grade- early childhood and have a primary disability. This data is managed by MDE.

GED Results: GED results include individuals who have passed the General Educational Development Test and received the State of Minnesota GED diploma. Individuals who take the GED are not currently enrolled in high school and do not have a high school diploma. In addition, test takers must be at least 19 years of age or at least 16 and have obtained an age waiver. GED results are based on a group of five subject tests which, when passed, certify that the taker has academic competencies similar to many of those required of a Minnesota high school graduate. This data is managed by MDE.

Postsecondary Enrollment: Fall term enrollment data collected from all Minnesota public and private postsecondary institutions, including but not limited to enrollment activity, program of enrollment, student level, student demographics, instructional activity, and secondary school information. This data is managed by OHE.

Postsecondary Completions: Degrees and other awards conferred data including information on degrees and other formal awards (diplomas or certificates) conferred to students upon successful completion of a program of study. This data is managed by OHE.

Institutional Characteristics: The Institutional Characteristics survey is administered by the U.S. Department of Education and provides general information about postsecondary institutions. Data collected include: Institution address, telephone number, website, educational offerings, mission statements, control/affiliation, award levels, calendar system, and admissions requirements. Inclusion of the institutional characteristics data in SLEDS is managed by OHE.

U.S. Higher Education Enrollments and Completions (National Student Clearinghouse): Data on national higher education enrollments and completions is collected by the National Student Clearinghouse and provides information about the enrollment activity and degrees conferred by postsecondary institutions in the United States. Inclusion of the National Student Clearinghouse data in SLEDS is managed by OHE.

Unemployment Insurance Wage Records: Data provided by all employers in Minnesota covered by Unemployment Insurance law. Data is provided quarterly and contains the names. Social Security numbers, wages, and hours of workers at each employer location. This data is managed by DEED.

Employer Detail: Data on all Minnesota businesses that describes their location, staff size, and primary industry. We use data from the North American Industrial Classification System, [NAICS](http://www.census.gov/eos/www/naics/) (<http://www.census.gov/eos/www/naics/>). This data is managed by DEED.

Workforce Training Participant Data: Data on individuals who participate in workforce training programs. Data includes individual characteristics, and services provided. This data is managed by DEED.

Definitions

1. **Contributing State Agencies:** Refers to the three state agencies with primary responsibility for SLEDS, including MDE, OHE, and DEED. Also included are the respective programs operated by the state agencies (e.g. Adult Basic Education operated by MDE).
2. **Data:** Categories of data in SLEDS ordered from most sensitive to least sensitive.
 - **Individual-Level Data:** Data on unique individuals.
 - **Identifiable Linked Data:** Original data from the contributing state agencies or partner data providers which are linked using personally identifiable information.
 - **Personally Identifiable Information (PII):** Data that identifies the individual. For the purposes of education records, PII is defined by federal law as information that includes, but is not limited to a student's name; the name of the student's parent or other family members; the address of the student or student's family; a personal identifier, such as the student's Social Security number, student number, or biometric record; other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name; other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; and information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.
 - **De-Identified Data:** Individual-level data that have enough personally identifiable information removed or obscured so that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify the individual. De-identified data will have a re-identification code that allows the recipient to match information received from the same source.
 - **Re-identification Code:** A re-identification code enables an authorized researcher to return to the source of de-identified data and match the de-identified data to the source records. It is used when a researcher wants to link SLEDS data to additional data or refer to the original source data.
 - **Anonymized Data:** Anonymized data are individual-level data that have been de-identified and do not include a re-identification code and cannot be linked back to the original record system or other data.

- **Summary Data:** Statistical records and reports aggregated from data on individuals in a way that individuals are not identified and from which neither their identities nor any other characteristic that could uniquely identify an individual is ascertainable.
3. **Data Mart:** Prepackaged data sets and reports.
 4. **Data Sharing Agreement:** Statement signed by the contributing state agencies and one or more parties seeking to share data that outlines the purposes of the data sharing, legal restrictions, conditions and violations.
 5. **Data Usage Agreement:** Statement outlining the appropriate uses of the data, which requires each user with access to SLEDS data to accept the conditions of use before being granted access to data or reports.
 6. **Directory Information:** For the purposes of education records, federal law defines directory information as information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed. Directory information includes, but is not limited to, the student's name; address; telephone listing; electronic mail address; photograph; date and place of birth; major field of study; grade level; enrollment status (e.g., undergraduate or graduate, full-time or part-time); dates of attendance; participation in officially recognized activities and sports; weight and height of members of athletic teams; degrees, honors and awards received; and the most recent educational agency or institution attended.
 7. **Education Records:** Records that are: (1) directly related to a student; and (2) maintained by an educational agency or institution or by a party acting for the agency or institution.
 8. **MARSS Number:** Minnesota Automated Reporting Student System; Unique K-12 identification number assigned by MDE to each K-12 student.
 9. **Minnesota P-20 Education Partnership:** The Minnesota P-20 Education Partnership is a voluntary organization made up of the statewide education groups in Minnesota, plus others from government, business, and other private sectors. Pursuant to its charter, the Partnership advises the contributing state agencies with regards to the governance of SLEDS.
 10. **MN.IT Services:** The state agency responsible for setting information technology (IT) direction, standards and policies for the State of Minnesota, managing oversight and compliance of those standards, and providing IT services to all Minnesota state agencies.
 11. **Partner Data Providers:** Organizations that provide data to a contributing state agency and agree to have this data used for or re-disclosed to SLEDS. A list of the current Partner Data Providers can be found on the SLEDS website.

12. **P20W:** refers to the overarching IT system of linked data serving Minnesota's three data initiatives, including Early Childhood Longitudinal Data System (EC LDS), Statewide Longitudinal Education Data System (SLEDS), and Workforce Data Quality Initiative (WDQI).
13. **Research Partners:** Individuals or organizations not categorized as contributing state agencies or partner data providers who have received authorization for research using SLEDS data.
14. **SLEDS:** Statewide Longitudinal Education Data System; refers to the data system specifically using linked data from P20W about pre-kindergarten to K-12 education to higher education to workforce for informing education and workforce policy.
15. **SLEDS Coordinator:** Staff person at a contributing state agency responsible for coordination and management of SLEDS-related activity for the agency.
16. **SLEDS Data Advisory Committee:** The Data Advisory Committee members shall advise SLEDS with regard to technical expertise about data collection, data structure, data security and protocols for maximizing validity and reliability of SLEDS data. Membership of the SLEDS Data Advisory Committee is set by the Minnesota P-20 Education Partnership charter.
17. **SLEDS Executive Committee:** The Executive Committee is comprised of the commissioners or their designees of the three contributing state agencies having responsibility for SLEDS. This group is the final decision making body of SLEDS.
18. **SLEDS Governance Committee:** The Governance Committee members advise the contributing state agencies in regard to SLEDS-related research and evaluation to inform data-driven decisions and policy formation. This committee advises on additional data elements to be added to SLEDS, data security protocols, appointment of members to the Research Committee and Data Advisory Committees, approval of requests for accessing data, and assurance of access to public data in accordance with state and federal privacy laws. Membership of the SLEDS Governance Committee is set by the Minnesota P-20 Education Partnership charter.
19. **SLEDS Research Committee:** The Research Committee members advise SLEDS with regard to data system access, research and evaluation proposals, research methodologies, and protocols for maximizing validity and reliability of SLEDS data. Membership of the SLEDS Research Committee is set by the Minnesota P-20 Education Partnership charter.
20. **Source System ID:** Refers to the ID used on individual person records by the data provider or state agency when submitting data to SLEDS. Where approved this ID allows new data to be linked to existing data or to refer to the original data source.

21. **Sponsored Research:** External requestors are designated as “sponsored research” if one or more contributing state agencies or partner data providers is supportive of its use of SLEDS data and provides a written statement of sponsorship as part of the requestor’s Data Access Request.
22. **Suppression Rules:** Analytic techniques used for appropriately protecting private or confidential data. Methods involve removing data (e.g., from a cell or a row in a table) to prevent the identification of individuals in small groups or those with unique characteristics. This method may result in very little data being produced for small populations, and it usually requires additional suppression of non-sensitive data to ensure adequate protection of personally identifiable information. Suppression rules may apply to all summary reports or may apply to specific reports based on the combination of data elements included. The SLEDS Research and Data Advisory Committees have agreed that suppression of cell sizes less than 10 individuals be used for public reporting. Best practices for data suppression for the purposes of appropriately protecting private or confidential data were issued by the U.S. Department of Education in 2011 (NCES 2011-603).

Maintaining the Privacy (Security) of Individual Information

There are many methods used to secure the privacy of individual-level data in SLEDS both at the system and user level.

MN.IT Services uses various procedures and security measures to ensure the confidentiality of an individual’s records collected and maintained by SLEDS, including but not limited to:

- Assigning a unique SLEDS identification number to each individual,
- Managing Levels of Access that limit who may have access to data and for what purposes,
- Masking data to ensure that the confidentiality of personally identifiable information (PII) from individual records is maintained in all public reporting,
- Developing and maintaining a list of personnel who have access to personally identifiable student information through authentication and internal links,
- Implementing and maintaining appropriate administrative, technical, and physical safeguards that prevent any collection, use or disclosure of, or access to electronically maintained or transmitted individual records in SLEDS, and
- Ensuring all staff with access to SLEDS data understand the sensitivity and classification of the data and follow all requirements to protect the data from unwanted disclosure.

Contributing state agencies use various procedures and security measures to ensure the confidentiality of an individual’s records collected and maintained by SLEDS, including but not limited to:

- Training of any state agency and affiliated MN.IT personnel collecting and/or using personally identifiable information about the proper use of that information in accordance with this policy, Minnesota Government Data Practices Act (MGDPA), Family Educational Rights and Protection Act (FERPA), and all applicable state and federal laws and policies,
- Enforcing a code of conduct for state employees, and
- Overseeing and managing all SLEDS-related work, policies and procedures to ensure compliance with data security standards, best practices, and federal and state laws.

Levels of Access

SLEDS data must be consistently protected in a manner commensurate with its sensitivity and critical nature. The following levels of access describe the data available and have been developed to protect the privacy of individuals. A complete list of individuals with access to SLEDS by level will be maintained by MN.IT Services and the contributing state agencies. Access is approved by appropriate leadership as defined for each access level. For each access level, approved staff must fulfill training requirements established by MN.IT and the SLEDS Executive Committee. The access levels listed below are in the order of the most restrictive to the least restrictive:

Level 1A – allows specific MN.IT staff, including those housed at contributing state agencies, to read and write to all records and fields in the P20W database. This access level is only permitted to a minimal number of authorized staff members who operate or manage the data system or are responsible for maintaining the accuracy and security of the data in the performance of their duties. Approval of access is granted by the appropriate contributing state agency commissioner or his/her designee and the OHE/MDE Chief Information Officer upon signing of the appropriate data sharing agreements.

Level 1B – allows one agency staff person (non MN.IT) access to all records and fields within the identifiable linked data in order to manage the P20W data system, manage reporting from the data system or maintain the accuracy and security of the data in the performance of their duties. The state agency's commissioner or designee approves access for the designated individual and signs the appropriate data sharing agreements before access is granted. Approval by the OHE/MDE Chief Information Officer is also required.

Level 2 – allows a minimal number of authorized DEED, MDE and OHE staff to access all records and fields of the SLEDS de-identified data. The requesting agency's commissioner or designee approves access for designated individuals and signs the appropriate data sharing agreements before access is granted. Suppression rules must be utilized by the researcher in production of summary level reports.

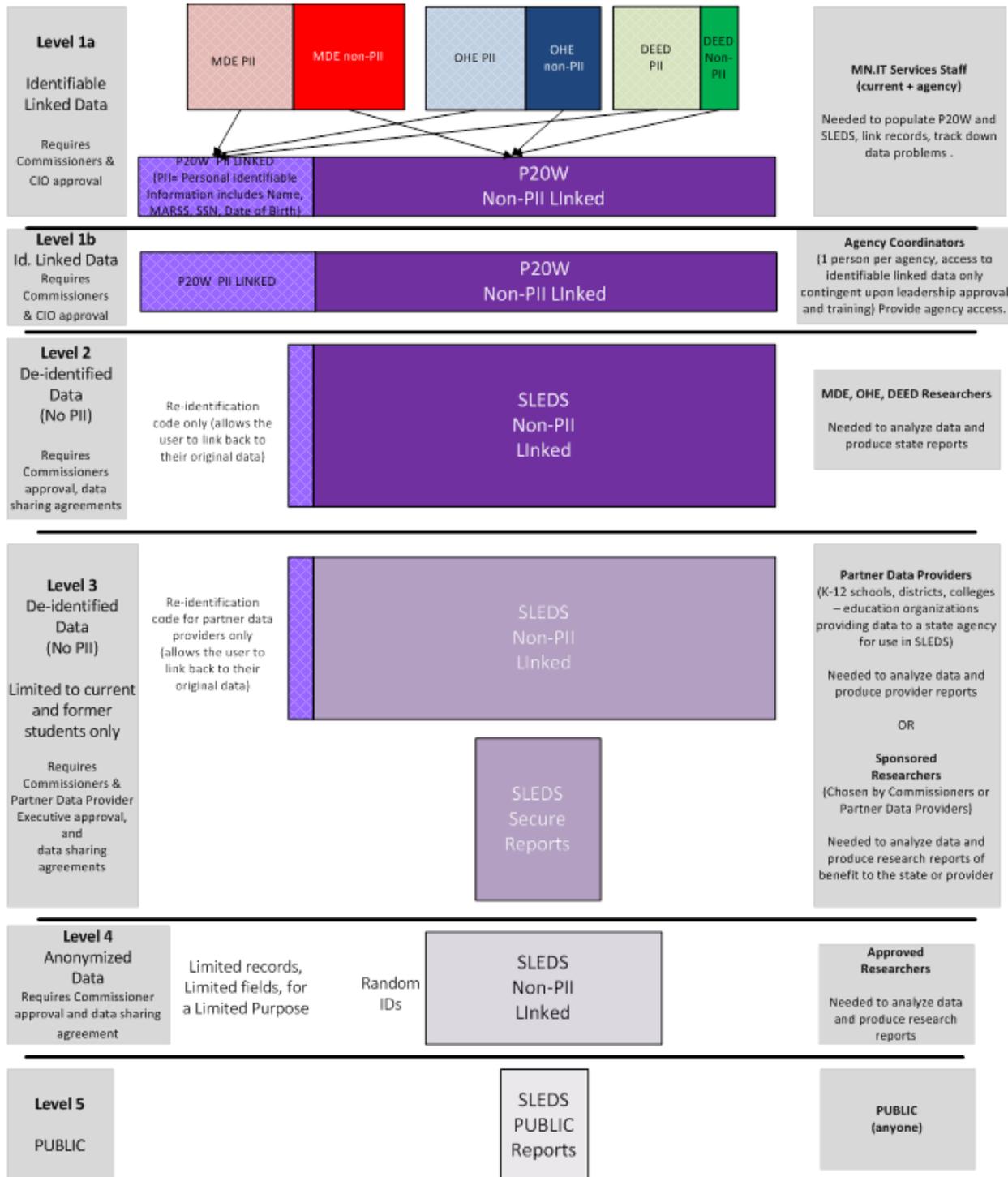
Level 3 – allows access for designated staff to SLEDS de-identified data and secured reports consistent with best practices, state and federal law. For approved research projects (partner data provider and sponsored researchers) access to data will be provided by data marts. Approval of access is granted by the contributing state agencies upon recommendation of the SLEDS Research Committee. Staff from

partner data providers must also have approval from their organization's executive and sign the appropriate data sharing agreements before access is granted. Suppression rules must be utilized by the researcher in production of public reports.

Level 4 – allows for access to anonymized SLEDS data in data marts to produce public reports. Suppression rules will be utilized with the use of data marts so that information is not revealed about individuals in a particular group. Approval of access is granted by the contributing state agencies upon recommendation of the SLEDS Research Committee. Users must be approved by the contributing state agencies and sign a data sharing agreement or data usage agreement before access is granted. Suppression rules must also be utilized by the researcher in production of summary level reports.

Level 5 – allows access to the general public for viewing standard summary SLEDS data. Requests for new public reports can be made to a SLEDS Coordinator.

Figure 1. Levels of Access to Data



Record of Access

Data security standards and requirements of state and federal law mandate that contributing state agencies maintain a record of each request to and each disclosure of personally identifiable information from SLEDS. Such records must be maintained as long as the data are maintained, include the parties who have requested or received the information, and include the legitimate interests of the parties in receiving the information.

Unauthorized Access

A state agency that collects, creates, receives, maintains, or disseminates private or confidential data on individuals must disclose any breach of the security of the data following discovery or notification of the breach.

A “Breach of the Security of the Data” means unauthorized acquisition of data maintained by SLEDS. Good faith acquisition of government data by an employee, contractor, or agent of a state agency for the purposes of the state agency is not a Breach of the Security of the Data, if the government data are not provided to an unauthorized person.

“Unauthorized acquisition” means that a person has obtained data without the informed consent of the individuals who are subjects of the data or statutory authority and with the intent to use the data for nongovernmental purposes.

In the event of a “Breach of the Security of the Data” or possible “Breach of the Security of the Data” involving individual records or aggregate and distributional reporting of individual records disclosed for purposes of SLEDS, contributing state agencies will notify MN.IT Services as described in the standard (Enterprise Information Security Incident Management Standard 2010-01); notify the duly authorized representative of state agencies; notify the Governance Committee for the SLEDS; and notify any individual whose private or confidential information was, or is reasonably believed to have been, acquired by an unauthorized individual as required by Minn. Stat. §13.055. The contributing state agencies and MN.IT will work together to monitor and respond to privacy and security incidents that do not rise to the level of a breach of security, in order to improve systems and prevent breaches.

Rights of Subjects of Data to Inspect and Review Data and Records

In compliance with state law, an individual who is the subject of stored private or public data on individuals may request to be shown the data without any charge and, if desired, be informed of the content and meaning of that data. In compliance with federal law, parents and eligible students have the rights to inspect and review education records. All records within SLEDS are managed by MDE, OHE and DEED and

as such those agencies are jointly responsible developing a policy for responding to all requests for access to SLEDS data and records in accordance with federal and state law.

Legislation Governing Data Sharing and Data Privacy

The majority of data in SLEDS is classified as private data by Minnesota statute. Private data can be used as necessary by the agencies that collect the data or have statutory authority to use the data. Private data cannot be disclosed except in specific situations. Federal regulations provide additional limitations to the use of certain data. Individuals found in violation of federal or state law or resultant policies and procedures are subject to consequences as documented in the Minnesota Government Data Practices Act (MGDPA), Family Educational Rights and Privacy Act (FERPA), and all data sharing and usage agreements for SLEDS.

Minnesota Government Data Practices Act (MGDPA)

The Minnesota Government Data Practices Act (MGDPA), Minnesota Statutes Chapter 13, asserts that all government data are public data unless classified otherwise. Public data can be disclosed to anyone for any reason. Private data, as designated under Minnesota law, may be collected, stored, used, or disseminated by government entities if the government entity is authorized to do so by state, local, or federal law (Minn. Stat.§ 13.05 sub.4(b); the individual subject or subjects of the data have given their informed consent; the data are being discussed at a meeting open to the public (see Minn. Stat.§13D.05). The majority of data in SLEDS are classified as private data, meaning their disclosure is limited to that authorized in statute. The use and preparation of summary data is permitted under Minn. Stat.§ 13.05 sub.7.

Education Data

In general, education data are classified as private under state law in Minnesota Statutes, 13.32, subdivision 1. "Educational data" means data on individuals maintained by a public educational agency or institution or by a person acting for the agency or institution which relates to a student. Pursuant to Minn. Stat.§ 13.32, subd. 11 the Minnesota Department of Education and the Minnesota Office of Higher Education have the authority to share educational data in order to analyze instruction in school districts for the purposes of improvement.

Adult Basic Education

Minn. Stat.§ 13.32, subd. 3(m) allows for the sharing of Social Security Numbers of students in the Adult Basic Education program with the Minnesota State Colleges and Universities and the Department of Employment and Economic Development for specified purposes.

Workforce and Training Data

Minn. Stat. § 13.47 allows for employment and training data to be shared among providers to determine eligibility, and coordinate and improve services.

Unemployment Insurance

Data collected for administering unemployment insurance benefits, including wage data is private data with limited exceptions for disclosure under Minn. Stat. § 268.19.

Family Educational Rights and Privacy Act (FERPA)

In compliance with the Family Educational Rights and Privacy Act, data for use in P-20W data systems such as SLEDS, requires that state agencies and partner data providers specify the conditions of use of data prior to inclusion. The conditions of use must include an anticipated data destruction date.

FERPA generally requires written consent of a parent or eligible student before an educational agency or institution discloses personally identifiable information. However, there are certain limited conditions in which prior consent is not required to disclose information (34 CFR Part 99.31).

These conditions include, but are not limited to, certain disclosures:

- To other school officials within the agency or institution determined to have legitimate educational interests
- To officials of another school, school system, or postsecondary institution where the student seeks or intends to enroll or is enrolled for purposes of the student's enrollment or transfer
- To authorized representatives of: 1) the Comptroller General of the United States; 2) the Attorney General of the United States; 3) the Secretary of the U.S. Department of Education; or 4) state and local educational authorities
- In connection with financial aid for which the student has applied or received
- To organizations conducting certain types of studies for, or on behalf of, educational agencies or institutions
- If the information disclosed is designated as "directory information", or
- If the information disclosed has been stripped of all personally identifiable information and determined that a student's identity is not personally identifiable after taking into account other reasonably available information

For more information on the conditions under which prior consent is not required to disclose information, please see Title 34, §99.31, of the Code of Federal Regulations for FERPA. Organizations and individuals found to be in violation of FERPA shall be prohibited from accessing information from SLEDS for a period of five (5) years.

Destruction of Data

Any entity receiving SLEDS de-identified or anonymized data must destroy such data when it is no longer needed within the specified study time period or for the purpose for which the study was conducted. The manner of destruction shall protect the confidentiality of the information, and include the purging of all copies from computer systems. The SLEDS Coordinators must receive written confirmation of the method and date of destruction of data disclosed from SLEDS.

Section 2 - Procedure for Requesting Access to SLEDS

Access to SLEDS data requires all requesters, including researchers associated with contributing state agencies or partner data providers, must submit a completed *Data Access Request*.

2.1 Types of Requests

Contributing State Agency request

Contributing state agency researchers may request access to de-identified data (level 2 access, level 3 access) or anonymized data (level 4 access) for the purposes of research and analysis using SLEDS data as outlined by the Data Access Request Process beginning in section 2.2 of this document. Access to SLEDS data requires the requester agree to provisions set forth in the *Data Sharing Agreement* and complete the required data privacy and data security training prior to data access being granted.

Partner Data Provider request

Partner data provider researchers may request access to de-identified data (level 3 access) or anonymized data (level 4 access) for the purposes of research and analysis using SLEDS data as outlined by the Data Access Request Process beginning in section 2.2 of this document. Access to SLEDS data requires the requester agree to provisions set forth in the *Data Sharing Agreement* and complete the required data privacy and data security training prior to data access being granted.

External request – Sponsored research

External requestors are individuals or organizations who have research and/or academic credentials or associations. They are not associated with a contributing state agency or partner data provider. External requestors are designated as “sponsored research” if one or more contributing state agencies or partner data providers is supportive of its use and provides a written statement of sponsorship as part of the requestor’s Data Access Request. An example of an external request for sponsored research would be TRiO programs requesting postsecondary outcomes of program participants as required for federal funding; such research is supported by the Minnesota Office of Higher Education. External sponsored researchers may request access to de-identified data (level 3 access) or anonymized data (level 4 access) for the purposes of research and analysis using SLEDS data as outlined by the Data Access Request Process beginning in section 2.2 of this document.

Role of Sponsors

The role of sponsor is to:

- Provide a written statement that the requested research will contribute to the work of a contributing state agency or partner data provider and cannot be done using public research products,
- Participate in the Data Access Request development process,
- Provide subject matter expertise and assist with analysis, as appropriate, during the course of research, and
- Assist in assuring that the results of research are shared with appropriate stakeholders.

Sponsor information should be included in the Data Access Request.

Access to SLEDS data requires the requester agree to provisions set forth in the *Data Usage Agreement* or formal *Data Sharing Agreement* and complete the required data privacy and data security training prior to data access.

External request

External requestors are individuals or organizations who have research and /or academic credentials or associations. They are not associated with a contributing state agency or partner data provider. External requestors may be granted access to anonymized data (level 4 access) or summary reports (level 5 access).

Public request

Summary reports (level 5 access) will be made available on the SLEDS website. Requests to create new summary reports can be made to a SLEDS Coordinator in writing and do not require a Data Access Request. Requests for new summary reports may be subject to fees as determined by the contributing state agencies. An example of a public request would be a media request for data on postsecondary participation rates of high school graduates by school district.

2.2 SLEDS Data Access Request Information

This section reflects policies, practices and templates adopted by contributing state agencies, the Minnesota P-20 Education Partnership, and the SLEDS partner data providers to effectively respond to requests for data access. These procedures reflect sound principles set forth by the U.S. Department of Education, U.S. Department of Labor, other states, and the education, workforce and research community, for managing the flow of data, establishing research priorities, monitoring appropriate use, protecting privacy and ensuring that research efforts are beneficial to the state of Minnesota, contributing

state agencies and partner data providers. All applicants requesting non-public data must submit a Data Access Request to be approved for access to SLEDS.

Roles and responsibilities

SLEDS Coordinators are charged with coordination and management of the Data Access Request Process. All requests for data access are received by a SLEDS Coordinator and forwarded to the SLEDS Research Committee for review and approval. All communication with the requestor is the responsibility of the SLEDS Coordinators.

The SLEDS Research Committee functions as a decision-making body and recommends approval or denial of a data access request. The SLEDS Research Committee recommends approval of access to SLEDS based on criteria authorized by the SLEDS Governance Committee. The SLEDS Research Committee is not an Institutional Review Board. The role of the SLEDS Research Committee is to screen data access requests to ensure they meet the criteria recommended by the SLEDS Governance Committee.

The SLEDS Governance Committee advises the SLEDS Executive Committee on standards for approving or denying access to SLEDS data.

The SLEDS Executive Committee has legal responsibility for approving access to SLEDS data and for the managing and securing the SLEDS data system.

Guidelines for Conducting SLEDS Research

Guidelines for the SLEDS Research Committee when reviewing requests for using SLEDS data are the following:

1. The study must involve analysis of transitions between systems or between providers within a system.
2. The study must be in alignment with state priorities.
3. The study must have the potential to make a definite contribution to contributing state agencies and partner data providers (e.g. study on impact of advising and college prep services to students at low-income public schools on high school graduation and college participation).
4. The researchers must use sound research design and have the potential for successful completion.
5. The project must comply with ethical standards for research in education and with all regulations set forth in federal and state law, particularly as they pertain to privacy of data on individuals.

Sensitive Data Elements

Some SLEDS data elements may be classified as “sensitive” based on “potential harm when used in contexts other than their intended use” per National Information Standards and Technology Special Publication 800-122 (2010). These classifications are noted in the data dictionary. Access to sensitive data elements may be limited in order to prevent potential harm or the identification of individuals as required by state and federal regulations. Access to sensitive data elements requires that the researcher submit a justification for inclusion of each requested data element as part of the Data Access Request.

Sensitive Data Elements include but are not limited to:

- K-12 Enrollment: Disability category, disability type, Homeless status, Migrant status
- Postsecondary Enrollment: Institution name, Disability category, Citizenship status

Qualifying FERPA Exception

Requests for personally identifiable information must demonstrate that such information is required for purpose(s) of the study. In addition, requests must identify the qualifying FERPA exception allowing for personally identifiable information to be disclosed.

- **Studies Exception** allows for the disclosure without consent of personally identifiable information (PII) from education records to organizations conducting studies “for, or on behalf of,” schools, school districts, or postsecondary institutions. These studies can only be for the purpose of developing, validating, or administering predictive tests; administering student aid programs; or improving instruction.
- **Audit or Evaluation Exception** allows for the disclosure of personally identifiable information (PII) without consent to authorized representatives of the FERPA permitted entities including Comptroller General of U.S., U.S. Attorney General, U.S. Secretary of Education, and 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 of said education programs (audit, evaluation, or enforcement or compliance activity).

Human Subject Review

The SLEDS Research Committee shall ensure that data privacy and security standards established comply with standards for the use of human subjects. However, the SLEDS Research Committee is not an Institutional Review Board.

Cost Sharing

In anticipation of the number of data access requests received by SLEDS, the SLEDS Executive Committee has determined that the costs of preparing data related to data access will be passed onto the researchers or other entities requesting data.

Cost estimates are based on the standard salary of the IT programming staff members who perform this type of work, currently \$70 per hour. SLEDS does not share costs related to data access if the request involves eight hours or less of SLEDS staff time.

The SLEDS Executive Committee may choose to waive all or a portion of the costs associated with preparing data for a data access request if the researcher or other entity is unable to pay the costs, or if the SLEDS Executive Committee determines that the data access request will result in a significant mutual benefit to the contributing state agencies that warrants waiving IT-related costs. Each data access request is reviewed independently by the SLEDS Research Committee.

This policy is consistent with the Minnesota Government Data Practices Act, which authorizes government entities to charge requesters for certain costs related to accessing government data.

Timeline for Data Access Request Review

Data Access Requests are reviewed on a monthly basis. The initial review of access requests will take 6-8 weeks and the entire approval process is likely to take 4-6 months, depending on the quality, type of request, and number of data elements requested.

2.3 SLEDS Data Access Request Requirements

For Data Access Requests to be considered, researchers must submit a complete application.

Step 1: Submit a Complete Data Access Request

Each organization or individual requesting access to SLEDS must submit a completed *Data Access Request*. Requests may be submitted via the SLEDS web interface. Submission of the Data Access Request requires the requester acknowledge data privacy statutes set forth by FERPA, MGDPA, SLEDS conditions of use, and the penalties for violating the stated obligations. The requested data may only be used for the purpose of the research or study proposed within the timeframe requested. To request the same or different data for another purpose, a new *Data Access Request* must be submitted. SLEDS data is not to be used for survey purposes.

A Data Access Request must include:

1. Researcher contact information
2. Research project title
3. Research project abstract describing the study including purpose of research and a description of its value to state policy, contributing state agencies, and partner data providers
4. Qualifying FERPA exception, if requesting personally identifiable data
 - school official with legitimate educational interest
 - studies for, or on behalf of educational agencies or institutions to: (A) Develop, validate, or administer predictive tests; (B) Administer student aid programs; or (C) Improve instruction (34 CFR 99.31(a)(6))
5. Theoretical background including references
6. Description of the study which must include the following:
 - 1) Hypotheses or specific research questions to be addressed
 - 2) The cohort or population to be studied
 - 3) The data elements requested, including specific justification for inclusion of sensitive data elements, and
 - 4) A description of the methodology and analysis you propose to perform
7. Any statement of sponsorship
8. A list of all funding sources and budget for the study
9. A time frame for completion
10. A signed statement of compliance with the SLEDS data security policy

Data Access requests should be uploaded via the SLEDS Researcher website when available. Requests will be prescreened by a SLEDS Coordinator to ensure it includes all required information. If any information is missing, the requester will be notified that the request is on hold until required information is submitted.

Step 2: Review by coordinators

In order to ensure clarity in requests, SLEDS coordinators will work with MN.IT Services to estimate fees and time required for fulfilling a Data Access Request. Upon review of this information with the requestor, SLEDS Coordinators will confirm the requestor's interest and forward the request to the SLEDS Research Committee

Step 3: Review by the SLEDS Research Committee

The SLEDS Research Committee shall review completed *Data Access Requests*.

Request Review Process

Once a completed *Data Access Request* is received, the SLEDS Research Committee will score the request by rating the following elements:

1. Analysis of transitions between systems or between providers within a system
2. Addresses state priorities as defined by the SLEDS Governance Committee
3. Have the potential to make a definite contribution to education and workforce research
4. Quality and technical adequacy of the study design, evidence of research and writing competence, and appropriateness of the data analyses
5. Have the potential for successful completion
6. Probability of compliance with ethical standards for research in education and with all regulations set forth in federal and state law, particularly privacy of data on individuals

The SLEDS Research Committee will review the proposal and make the recommendation for approval or revision. Upon completion to the review process, designee scoring and comments shall be forwarded to the SLEDS Executive Committee.

Step 4: Final Approval Process

After reviewing the request and the recommendation from the SLEDS Research Committee, the SLEDS Executive Committee may respond to the request in one of three ways:

1. **Approve the request:** Upon approval of the Data Access Request, the requester will be contacted by a SLEDS Coordinator of the approval.
2. **Invite revisions to the request:** In some instances, the SLEDS Executive Committee may request additional information or ask that the requester revise the Data Access Request in response to comments, questions, or suggestions from Research Committee members or to ensure compliance with data privacy statutes and the SLEDS data security policy. A SLEDS Coordinator will contact the requester with the Committee's revision request.
3. **Deny the request:** While it is the policy of the SLEDS Executive Committee to facilitate access to SLEDS data, the SLEDS Executive Committee may deny a Data Access Request which fails to meet the criteria established, violates data privacy law or SLEDS contractual obligations, if the requester refuses to

comply with terms of use, data sharing agreements, or SLEDS data security policy, or if the requestor has violated data privacy law or refused to comply with applicable policies and procedures in the past.

Acceptance of the terms of use

Once approved, permission to access the SLEDS data requires the requester to complete an online *Data Usage Agreement* or formal *Data Sharing Agreement* prior to data access.

Data Transfer

The approved data will be made available by MN.IT Services to the requester by secure means.

Step 5: Completion of Research

Completion of research requires the requester to submit research findings and comply with data destruction requirements, if applicable.

Submission of Research Findings

The *Data Usage Agreement* and *Data Sharing Agreement* requires that all requesters provide a SLEDS Coordinator with a paper and electronic report of final results no less than 30 days prior to publication of the study. The report will be forwarded by a SLEDS Coordinator to the SLEDS Research Committee, research sponsors, and the contributing state agency commissioners. After publication, the SLEDS Coordinator will forward the report to the SLEDS Governance Committee and the SLEDS Document Library. Failure to submit a final report jeopardizes approval of future proposals. Publications emanating from studies using SLEDS data should acknowledge the contributions of SLEDS.

Data Destruction

Upon completion of the study time frame, each requester will be notified by the designated SLEDS coordinator that the study period has ended and that the data must be destroyed. The researcher must sign a compliance statement or send a letter to the agency coordinators that the data has been destroyed. If additional external data was submitted by the researcher for purposes of linking to SLEDS data, the SLEDS coordinator will issue a letter to the researcher that the data has been destroyed.

Report of Completed Research

It is the responsibility of the SLEDS Research Committee and the SLEDS Coordinators to provide the SLEDS Governance Committee, the SLEDS Executive Committee and the Minnesota P-20 Education Partnership with a report on completed research. The SLEDS Governance Committee shall determine the schedule for reporting.

Section 3 - Policy Authorization

This policy was adopted by the SLEDS Governance Committee, the Minnesota Department of Education, Minnesota Department of Employment and Economic Development, and Minnesota Office of Higher Education.

This policy is effective October 23, 2014.

Lawrence J. Pogemiller

Commissioner

Minnesota Office of Higher Education

Kevin McHenry

Assistant Commissioner

Minnesota Department of Education

Blake Chafee

Deputy Commissioner

Minnesota Department of Employment and Economic Development

Amendment to the SLEDS Data Access and Management Policy

This amendment provides the administrative **structure and process** for SLEDS partners to re-identify data from SLEDS in compliance with data security and other applicable policies, and state and federal law. The ability to re-identify data for contributing state agencies (Level 2 users) and partner data providers (Level 3 users) is authorized in accordance with the SLEDS Data Access and Management Policy, enacted October 2014 and governing state and federal data practices laws, and approved by the SLEDS Executive Committee in July 2016. This amendment clarifies the administrative process for obtaining and using re-identification.

Guidelines for SLEDS Re-identification Design

Re-identification of data from SLEDS must meet the following guidelines in order to maximize use and protect individual data:

1. Personally identifiable information (PII) does not reside, nor will it reside, within the SLEDS Data Warehouse. The SLEDS Data Warehouse was designed to contain only de-identified data.
2. However, state agencies and data providers that contribute data to SLEDS are authorized to reconnect de-identified data from SLEDS back to their source data for additional analysis that is approved by the SLEDS Executives Committee, and aligns with SLEDS guidelines for access to data and applicable state and federal laws governing the data.
3. Each state agency or data provider should only receive the PII from P20W which they contributed to P20W. Re-identification does not involve giving agencies or data providers additional PII which they didn't already have.
4. Effort to create, maintain, and use the re-identification system should be minimal. If the system is too complex, it won't be useful.

SLEDS Data Warehouse Reported Person Crosswalk Table

Re-identification can be done using a SLEDSDW Reported Person Crosswalk Table. The P20W Linking Process generates the P20W Reported Person Table in the P20W Operational Data Store (ODS). The P20W Reported Person Table contains all source data PII and the P20W Reported Person ID, with one record per instance of the person identified from the source data.

The P20W Linking Process will also create a SLEDSDW Reported Person Crosswalk Table for generating the SLEDS Reported Person ID which is associated with the person's records in the SLEDS Data Warehouse. This crosswalk table exists only in the P20W ODS and is the link between the de-identified SLEDS Reported Person ID and the original PII in the P20W Reported Person Table in the P20W ODS.

SLEDS Re-identification for Contributing State Agencies (Level 1B and Level 2 Users)

The process for re-identification of data files for contributing state agencies (Level 2 users) begins with MN.IT generating the SLEDSDW Reported Person Crosswalk Table at the end of the linking process. The SLEDSDW Reported Person Crosswalk is a subset of source data files with the SLEDS Reported Person ID appended to each record. MN.IT would then securely transfer these regenerated source data files to each agency's SLEDS Coordinator.

This design provides each agency with precisely the source data files and PII which they contributed, with the addition of the SLEDS Reported Person ID. An agency user approved to use re-identified data could then link their source data with the SLEDS Data Warehouse de-identified data using the SLEDS Reported Person ID. Level 2 users must work with their SLEDS Data Coordinator to use the SLEDSDW Reported Person Crosswalk Table for additional data analysis.

The SLEDS Reported Person ID is recreated each time the P20W linking process is rerun to generate the SLEDS Data Warehouse. Therefore, these regenerated source data files are only good for a specific version of the SLEDS Data Warehouse.

SLEDS Level 1B Approved Users (Limited to Data Testing & Validation)

SLEDS Coordinators from contributing state agencies may be granted access to re-identifying data as Level 1B users solely for the purpose of data testing and validation.

- Users currently have access to the full SLEDS Data Warehouse with SLEDS Person IDs
- Users will receive the SLEDS Re-identification Crosswalk table in their Movelt account, under the current authority provided Level 1B users
 - DEED Re-identified data sources include: Workforce Training (W1) and Employment/Wages
 - OHE Re-identified data sources include: Postsecondary Enrollment & Completion, and National Student Clearinghouse.
 - MDE Re-identified Data Sources include: K-12 Enrollment, Advance Placement, SAT/PSAT, ACT and IB.

- Re-identification Crosswalk table include SLEDS Person ID, PII, and selected record identification fields (e.g. data year). SLEDS Data Coordinators configure the exact list of fields added to the crosswalk table per data source.
- Crosswalk table must also include the crosswalk table generation date AND the data source release identifier (e.g. November 2014 P20W Data Release). Because every relinking regenerates SLEDS Person IDs, if a given data release has multiple relinked data releases, then there must be a sub release ID too.

SLEDS Level 2 Approved Users / Authorized State Agency researchers, upon request (Level 2 e.g. OHE Research staff)

Staff from contributing state agencies may be granted access to re-identifying data as Level 2 users solely for the purpose of approved SLEDS data requests.

1. Level 2 users must submit a request for re-identification of data along with their SLEDS Data Request. Re-identification requests must answer the following questions:
 - Why is re-identification of data needed?
 - What data will be linked using re-identification?
 - Why can't the research question be answered without re-identification?
2. Level 2 users have access to only the SLEDS data provided in response to their SLEDS Data Request. This may be handled using a researcher data mart.
3. Level 2 users will receive a SLEDS Re-identification Crosswalk table from a SLEDS Level 1B staff member upon approval of the request by the SLEDS Executive Committee.

SLEDS Re-identification Proposal for Partner Data Providers (Level 3 Users)

K-12 schools and districts, colleges and universities are authorized to link data from SLEDS with their internal data systems. The SLEDS Data Access & Management Policy identifies that these organizations may be granted access to re-identified data under SLEDS Data Access Level 3. Partner data providers may be granted access to re-identifying data as Level 3 users.

The process for re-identification of data files for partner data providers (Level 3 users) begins with MN.IT generating the SLEDSDW Reported Person Crosswalk Table at the end of the linking process. Level 3 users currently have access to SLEDS using SLEDS Secure Reports or approved SLEDS Data Requests. These data marts and data requests contain individual level data on current and former students.

In the short term, the SLEDS Coordinator at the associated state agency could create an extract of the SLEDSDW Reported Person Crosswalk Table for the Level 3 organization, limited to current and former students enrolled. In the long term, MN.IT should be able to extend the P20W configuration database to include partner data providers (Level 3 users) so that P20W could automatically regenerate source data files for just that organization and then securely transfer those files to the appropriate user.

SLEDS Level 3 Approved Users / Partner Data Providers, upon request (Level 3 e.g. College IR Director)

1. Level 3 users must submit a request for re-identification of data along with their SLEDS Data Request. Re-identification requests must answer the following questions:
 - Why is re-identification of data needed?
 - What data will be linked using re-identification?
 - Why can't the research question be answered without re-identification?
2. Level 3 users have access to only the SLEDS data provided in response to their SLEDS Data Request. This may be handled using a researcher data mart.
3. Level 3 users will receive a SLEDS Re-identification Crosswalk table from a SLEDS Level 1B staff member upon approval of the request by the SLEDS Executive Committee.

Amendment Authorization

This policy was adopted by the SLEDS Governance Committee, the Minnesota Department of Education, Minnesota Department of Employment and Economic Development, and Minnesota Office of Higher Education.

This policy is effective September 25, 2018.

Appendix A: Documents and Forms

A1. Data Sharing Agreement – Contributing State Agencies and MN.IT

- a. OHE – MN.IT Data Sharing Agreement
- b. OHE – MDE Data Sharing Agreement
- c. OHE – DEED Data Sharing Agreement

A2. Data Access Request Application, including Statement of Sponsorship

A3. Written Statement of Data Destruction Compliance

- a. Researcher to SLEDS
- b. SLEDS to Data Provider

Minnesota SLEDS Data Access Request Application

Overview

Date: Enter the date here

To: SLEDS Coordinators

(email completed application to the [SLEDS Coordinators](mailto:SLEDS.Support@state.mn.us) SLEDS.Support@state.mn.us)

From: Enter organization name here

Project Title: Enter project title here

(Insert Organization or Researcher name) requests access to de-identified student-level data residing in the Minnesota's Statewide Longitudinal Education Data System (SLEDS) for the purpose of conducting statistical research on (insert project description here).

1. Researcher contact information

Researchers listed should be those individuals who will have access to and responsibility for the data requested.

- Name: Please insert your name here.
- Organization: Please insert your organization here.
- Address: Please insert your address here.
- City, State, Zip: Please insert your city, state and zip here.
- Email: Please insert your email address here.
- Phone: Please enter your phone number here.

If more than one researcher, please list additional contacts below.

2. Research project title

Please insert the title of your research project here.

3. Abstract

Please insert an abstract of your research project here.

4. Theoretical background, including references

Please insert the theoretical background of the research project here. A full citation of references may be included in section 13.

5. Description of the study

Please insert a description of the study here.

6. Research questions

Please list your specific research questions here.

7. Cohort

Please describe the population you are seeking to study.

8. Methodology

Please describe the statistical methodology you will use to answer your research questions. Examples include descriptive statistics, correlations, regression, etc.

9. Statement of sponsorship? Yes No

Please indicate if you have received sponsorship from a SLEDS Contributing State Agency or Partner Data Provider by checking “yes” or “no”. For more information on sponsorship, please see appendix 1. If yes is checked, please send the statement of sponsorship (example letter provided in appendix 1) with the application.

10. Timeframe for completion

Please indicate the time frame for completing this research project.

11. Statement of compliance with SLEDS data security policy

By submitting this application, the applicant(s) agree with the following statement:

All researchers associated with this project agree to all provisions set forth in the Data Sharing Agreement and to complete all required data privacy and data security trainings prior to data access.

For your reference, the standard data sharing agreement can be found in Appendix 2.

12. Data Security

Please describe your plan for managing and limiting staff access to the data, and for maintaining the data in a secure way in compliance with the SLEDS data security policy.

13. References

Please insert citations used in theoretical background descriptions.

14. Data Elements

Please indicate the SLEDS data elements needed to answer the research questions by entering them in the table 1 template below.

Available data elements are found in the [SLEDS Data Dictionary](http://sleds.mn.gov/dataDictionary/) (<http://sleds.mn.gov/dataDictionary/>). Please refer to the [data interpretation guide](http://sleds.mn.gov/#research) (<http://sleds.mn.gov/#research>) for specific information and caveats related to data use.

Table 1: SLEDS Data Elements Request (Sample)

Line Number	Source Table	Variable Name	Variable Label	Variable Codes <i>(Please indicate if you would like all values or only specific values shown.)</i>
1 <i>(required for all requests)</i>	SLEDS	PERSON ID	Unique person identifier	All
2	K12 Enrollment	Status End	Status End	All
3	K12 Enrollment	Time ID	Last Day of Fiscal Year	Years 2006-2012
4	K12 Enrollment	Grade	Grade	All
5	K12 Assessment	Test Name	Test Name	Test reported for students if enrolled in grades 10-11
6	K12 Assessment	Subject	Assessment Test Subject	Test reported for students if enrolled in grades 10-11
7	K12 Assessment	Proficiency	Proficiency Level	Last test reported for students enrolled in grades 10-11

Letter of Sponsorship for SLEDS Research

Date:

To: SLEDS Data and Research Committee and SLEDS Governance Committee

From: <Contributing State Agency or Partner Data Provider Executive or Designee>

Re: Letter of Sponsorship for Example Research Study

The Contributing State Agency or Partner Data Provider supports the research request for Organization's study on (insert purpose), (insert project title). This research will advance the work of our organization by (insert outcome of research here). This research is only possible by the use of private data made available through SLEDS and could not be done using public records.

__ (signature) _____
Contributing State Agency or Partner Data Provider Executive

Date

Title

Organization

Address

City, State ZIP

Phone

Email

A3. Written Statement of Data Destruction Compliance

A3a. Researcher to SLEDS

Letter Confirming Data Destruction

Date:

To: SLEDS Coordinators

From: <Researcher>

Re: Letter Confirming Data Destruction for Example Research Study

The letter is to confirm the destruction of SLEDS data provided to Researcher for Organization's study on (insert purpose), (insert project title) pursuant to the Data Sharing Agreement between the Minnesota Office of Higher Education and Organization. Please let me know if you require further information.

_ (signature)
Researcher Name

Date

Title

Organization

Address

City, State ZIP

Phone

Email

Letter Confirming Data Destruction

Date:

To: <Researcher>

From: SLEDS Coordinators

Re: Letter Confirming Data Destruction for Example Research Study

The letter is to confirm the destruction of data provided to the Minnesota Office of Higher Education and MN.IT Services by Researcher for Organization's study on (insert purpose), (insert project title) pursuant to the Data Sharing Agreement between the Minnesota Office of Higher Education and Organization. Please let me know if you require further information.

_ (signature)

SLEDS Coordinator Name

Date

Title

Organization

Address

City, State ZIP

Phone

Email

SLEDS DATA SHARING AGREEMENT BETWEEN THE MINNESOTA OFFICE OF HIGHER EDUCATION AND THE ORGANIZATION

This Agreement is entered into by the **Minnesota Office of Higher Education (OHE)** and the **Organization (ORG)** for purposes of sharing data from the Statewide Longitudinal Education Data System (SLEDS) in a manner consistent with applicable federal and state laws and for research approved by the SLEDS Executive Committee. The data will be used by **the Organization** for the purpose of ...

The SLEDS is a linkable data repository to identify, organize, and analyze education and workforce data facilitating creation of summary reports to be created for students, parents and stakeholders. It will also create data analytic tools for education and workforce research and evaluation to provide timely and relevant information for policy and practice. SLEDS will help identify the most viable pathways for individuals in achieving successful outcomes in education and work, inform decisions to support and improve education and workforce policy and practice, and assist in creating a more seamless education and workforce system for all Minnesotans.

Parties

1. OHE is the state agency responsible for collecting data on students enrolling in and completing postsecondary education. OHE is a state educational authority and has corresponding authority and responsibility to evaluate postsecondary education in Minnesota.
2. OHE is the chair of the Minnesota P-20 Education Partnership SLEDS Governance Committee, the governing body for SLEDS, which includes leadership representatives from the contributing state agencies and provides additional oversight and direction for SLEDS activities in accordance with Minn. Stat. § 127A.70, subd. 2, Minn. Stat. § 116J.401, and Minn. Stat. § 13.32, subds. 6 and 11. OHE receives state general funds for operation and management of SLEDS.
3. **The Organization is ...**

Legal Authority for Data Sharing

1. OHE is authorized under the Family Education Rights and Privacy Act (FERPA) and Minn. Stat. § 13.32, subd. 3(e), to disclose otherwise private educational data regarding individual students to another entity in certain circumstances. OHE is a state educational authority as described in 34 C.F.R. § 99.31(a)(3). In accordance with 34 C.F.R. § 99.31(a)(6), FERPA permits state educational authorities to redisclose data received from local educational authorities without prior consent to an organization conducting

studies for or on behalf of educational agencies for the purpose of improving instruction. This Agreement complies with 34 C.F.R. §§ 99.31(a)(6) and 99.33(b). Finally, this Agreement complies with Minn. Stat. § 13.32, subd. 3(e) of the Minnesota Government Data Practices Act (MGDPA), which permits disclosure of private student data pursuant to FERPA.

2. SLEDS is governed by a separate data sharing agreement between OHE and MN.IT, the state agency responsible for providing information technology services, management, and security to Minnesota state agencies. That data sharing agreement governs expectations for data collected from the state agencies participating in SLEDS: OHE, the Minnesota Department of Education (MDE), and the Minnesota Department of Employment and Economic Development (DEED). Separate data sharing agreements with those agencies allows OHE to collect, manage, and use data from those agencies in SLEDS.
3. OHE is granted authority by the SLEDS Executive Committee to share data received from MDE and DEED for the purpose of research approved under agreements consistent with the SLEDS Data Access and Management Policy.
4. This data sharing agreement is also consistent with the SLEDS Data Access and Management Policy, which requires data sharing agreements for all access to SLEDS data.

Purpose and Scope

1. Data shared under this Agreement will involve merged data created in SLEDS originally provided by OHE, MDE, or DEED and includes de-identified individual level data for the purpose of
2. Data shared will be used to answer the following research questions: (research questions listed here)
3. Data elements to be shared are listed in Attachment 1.

Duties

1. OHE responsibilities. OHE will:
 - a. Provide to The Organization de-identified individual level data from SLEDS consistent with this Agreement and as described in Attachment 1, and
 - b. Create and maintain a secure method of transmission of data.
2. The Organization responsibilities. The Organization will:

- a. Conduct statistical research as described in the Purpose and Scope section of this Agreement.
- b. Reporting of Postsecondary Institution Data
 - i. The Organization shall conduct all research and reporting, including SLEDS, in a manner that does not permit identification of the institution providing the education records by individuals except where permission for release is granted to OHE by the postsecondary institution. Authorized representatives of the Organization are permitted to identify institutions solely to facilitate research purposes approved under this agreement but not for public reporting or public identification.
 - ii. For purposes of this section, *Summary Data* is defined as statistical records and reports aggregated from data on individuals in a way that individuals are not identified and from which neither their identities nor any other characteristic that could uniquely identify an individual is ascertainable.
 - iii. Permission for release of postsecondary institution identification pursuant to data shared under this Agreement is granted in the following circumstances:
 - 1. Summary data published by the Organization pursuant to state or federal mandate, including but not limited to Minn. Stat. §136A.121 Subd. 20, and Workforce Innovation and Opportunity Act (WIOA);
 - 2. Summary data approved as part of SLEDS web-based data tools including, but not limited to SLEDS mobile analytics; Graduate Employment Outcomes, published reports (e.g. *Getting Prepared 2016*) or other SLEDS branded research products developed by the Office of Higher Education, the Minnesota Department of Education or the Minnesota Department of Employment and Economic Development;
 - 3. Summary directory data, including enrollment counts, and awards conferred counts, and
 - 4. Summary data used by the Organization for internal planning and management and not for publication.
- c. Provide OHE's authorized representative with a paper and electronic report of final results no less than 30 days prior to publication,

- d. Understand and comply with all of the data practices provisions of this Agreement.

Data Practices Provisions

1. OHE and **The Organization** each agree to abide by the provisions of the Minnesota Government Data Practices Act, Minnesota Statutes 13.01 *et seq.*, and any and all other applicable state and federal laws governing the SLEDS data shared pursuant to this Agreement and all data, created, collected, received, stored, used, maintained, or disseminated by OHE under this Agreement. Each party is individually responsible for compliance with laws and regulations governing or affecting the collection, storage, use, sharing, disclosure and dissemination of private data.
2. **The Organization** agrees to comply with all applicable federal and state laws, statutes, and rules with respect to the protection of privacy, security and dissemination of the shared data. Nothing in this agreement may be construed to allow either party to maintain, use, disclose or share student information in a manner not allowed by federal or state laws. **The Organization** understands that personally identifiable information maintained by either party to the agreement is subject to the privacy and confidentiality provisions of federal and state statutes, rules and regulations, including, but not limited to, the Family Education Rights and Privacy Act (20 U.S.C 1232g); related federal regulations (34 C.F.R. Part 99); the Minnesota Government Data Practices Act, Minnesota Statutes 13.01 *et seq.*; and federal laws and regulations regarding students with disabilities (20 U.S.C. §1417 (c); 34 C.F.R. 300.32, 34 C.F.R. §§ 300.610-300.627)).
3. **The Organization** agrees to use the SLEDS data it receives only to the extent necessary to complete its approved research. **The Organization** will not use the individual-level data for any other purpose.
4. Data exchanged under this Agreement may not be duplicated, disseminated or used by **The Organization** for another purpose or program without the express written permission of OHE as approved by the SLEDS Executive Committee. All copies of data of any type, including modifications or additions to data from any source that contains information regarding individuals, are subject to the provisions of this Agreement in the same manner as the original data.
5. Data exchanged under this Agreement will be made available to **The Organization** by OHE through secure means as required under the SLEDS Data Access and Management Policy.
6. **The Organization** agrees that only those employees, contractors, and agents who need to have access to data provided under this Agreement because they are conducting

work directly related to approved research will have access to the data. **The Organization** agrees to provide OHE with a list of staff members currently assigned to the approved research upon request.

7. **The Organization** agrees that all employees, contractors, and agents who receive data provided pursuant to this Agreement, will agree in writing to comply with all applicable data practices, data privacy laws and regulations.
8. All employees, contractors, and agents of **The Organization** who have access to data shared under this Agreement will complete required data practices and data security training consistent with the SLEDS Data Access and Management Policy.
9. All employees, contractors and agents of **The Organization** who have access to the data shared under this Agreement will comply with all applicable federal and state laws with respect to the data shared under this Agreement.
10. **The Organization** agrees that all individuals having access to data under this Agreement are subject to adequate supervision to ensure compliance with applicable federal and state data practices law.
11. **The Organization** will use reasonable efforts to store and process all data collected, created, used, maintained, or disclosed in such a way that unauthorized persons cannot retrieve the information by means of a computer, remote terminal, or any other means. **The Organization** will use appropriate safeguards to prevent use or disclosure of private data on individuals by its employees, contractors, and agents, including but not limited to implementation of administrative, physical, and technical safeguards to reasonable and appropriately protect the privacy and integrity of individual-level data that it creates, receives, maintains or transmits under this Agreement.
12. **The Organization** will report any known data security or data privacy incidents to OHE as soon as they become known. For purposes of this Agreement, security incident means the unauthorized access, use, disclosure, modification, or destruction of information provided by SLEDS. Privacy incident means violation of the MGDPA or any other applicable state or federal data practices laws, including, but not limited to, improper and/or unauthorized use or disclosure of protected information and breach of security of information as defined by Minnesota Statutes, Section 13.055. This report must be made in writing and submitted to the authorized representatives after the security or privacy incident is discovered by **The Organization**.
13. **The Organization** will only disclose data in summary form for public reports.
14. **The Organization** will destroy data received under this Agreement when it is no longer needed for the purpose of the study that it was requested for or when the specified study time period has ended.

15. **The Organization** will use a secure method of destruction that prevents inadvertent release of any data and protects the privacy and confidentiality of the data before, during, or after the destruction process.
16. After **The Organization** has destroyed any data, **The Organization** will send a letter to the authorized representative that confirms the method and date of the data destruction.
17. Summary data and summary analyses created from SLEDS data are not subject to destruction requirements.
18. If OHE determines that **The Organization** has violated this Agreement, OHE reserves the right to request that **The Organization** immediately destroy all de-identified or anonymized data received under this Agreement.
19. OHE retains the right to conduct audits or other monitoring of **The Organization's** policies, procedures, and systems related to storage and analysis of SLEDS data. **The Organization** agrees to allow OHE reasonable access if OHE conducts any audit or monitoring.
20. **Liability.** No party will be liable for violations of any applicable laws, or the terms of this Agreement, indirectly or directly arising out of or resulting from, or in any manner attributable to the actions of the other party. The liability of a state agency is governed by the provisions of the Minnesota Torts Claims Act, Minn. Stat. § 3.732 and 3.736, *et. seq.*, and other applicable law.
21. **Transfer.** Neither OHE nor **The Organization** may assign its obligations under this Agreement, nor any part of its interest in this Agreement, to another party.
22. **Amendment.** Any amendments to this Agreement shall be in writing and shall be executed as an amendment to the Agreement. Data Access Requests approved by the SLEDS Executive Committee will be amendments to this Agreement.
23. **Cancellation.** This Agreement may be canceled by any party at any time, with or without cause, upon thirty (30) days written notice to the other parties. Each party specifically reserves the right to immediately cancel this Agreement should a party, in its sole discretion, determine that private or confidential student information has been released in a manner inconsistent with this Agreement or has not been maintained in a secure manner.
24. **Authorized Representatives.** OHE and The Organization designate a single authorized representative for purposes of maintaining the data sharing agreement and ensuring that it is properly enforced.

OHE authorized representative is Meredith Fergus, SLEDS Coordinator, (651) 259-3963.

The Organization's authorized representative is

Effective Dates. The terms of this Agreement shall take effect upon signature of both parties and will remain in effect until (research end date).

Signatures here.

Table 1 here

