

Data Sharing for Program Evaluation

Guidance on Sharing Student-Level Data While Protecting Student Privacy

This document is meant to share:

- Basic information with school districts about the language in federal regulations that allow districts to share and/or use data for “studies” and “audits or evaluations”; and
- High-level guidance and additional resources for districts interested in putting a data sharing agreement in place with a third-party researcher or program evaluator.

The document is divided into the following sections:

- Why Share Data for Program Evaluation?
- Federal Regulations on Sharing Student Education Records
- Recommended Steps and Considerations
- Additional Resources:
 - Data Sharing and Student Privacy
 - Data Sharing and Research
 - Ohio Department of Education Data Sharing Template
 - Data Sharing Template: Considerations for Districts Participating in School-Based Health Care

While the document includes some additional resources on developing strong research partnerships, this is not meant to be a primary focus of the document.

This information is being shared as a courtesy to local districts. Districts should consult their legal counsels about the proper use of this guidance prior to sharing any data with a third party for research and evaluation.

WHY SHARE DATA FOR PROGRAM EVALUATION?

Thoughtful, well-planned program evaluation can give districts the information they need to understand the strategies, activities or interventions that are contributing to improved student outcomes. Some types of rapid-cycle evaluations even enable districts to fine-tune student support strategies *while* they are being carried out, resulting in almost real-time opportunities for improvement.

While third-party research partners can supplement a district’s existing program evaluation resources with additional capacity and expertise, it is generally only through partnerships with districts or state education agencies that they have access to the kinds of data that will help them carry out a robust and meaningful program evaluation.

Beyond the inherent value of using data and evaluation to shine a light on what is working in district, the Every Student Succeeds Act (ESSA) (Section 8002) requires greater use of evidence-based strategies in addressing school improvement. By engaging in program evaluation work, districts are contributing to the growing evidence-base in education research.

FEDERAL REGULATIONS ON SHARING STUDENT EDUCATION RECORDS

The sharing and use of individual student education records is regulated by the [Family Education Rights and Privacy Act \(FERPA\) \(§34 CFR Part99\)](#).

Section §99.30 outlines the circumstances under which educational agencies are required to obtain parental consent prior to disclosure.

Section §99.31 outlines the circumstances under which prior consent is not required to disclose information. There are two exceptions under which prior consent is not required for disclosure:

- The “studies exception” allows for the disclosure of personally identifiable information (PII) to organizations conducting studies “for, or on behalf of” the educational agency.
- The “audit or evaluation exception” allows for the disclosure of personally identifiable information to authorized representatives of FERPA-permitted entities to audit or evaluate a federal- or state-supported education program or to enforce or comply with federal legal requirements related to an education program.

RECOMMENDED STEPS AND CONSIDERATIONS

1. **Learn more** about your responsibility to protect student privacy from national resources such as the U.S. Department of Education’s Protecting Student Privacy website. This website provides a wide range of resources for education agencies interested in understanding FERPA regulations and the impact of those regulations on student data collection, sharing and reporting.
2. **Consult your legal team early in the process.** Your legal team can help you understand your district’s existing policies and practices regarding data sharing. If your district does not have an existing process, your legal team can help you develop the right language for your district.
3. **Involve in your planning processes the IT and data staff** who will play a role if your district decides to share data with a third-party researcher. Who will help you decide which data to share? Who will transfer the data to the researcher? Who will address the researcher’s technical questions about the data?
4. With support from your legal and data teams, **develop the appropriate data sharing agreements.** Data sharing agreements outline the specific terms under which your district is agreeing to share the data with a third party; the data sharing agreement plays a significant role in addressing the technical details that will help ensure student privacy and data security.
 - a. The exact details and wording included in data sharing agreements may vary slightly from district to district. The U.S. Department of Education provides several resources to help you develop strong data sharing agreements, including:
 - i. [Guidance for Reasonable Methods and Written Agreements](#); and
 - ii. [Written Agreement Checklist](#).
 - b. Data sharing agreements also can document other, agreed-upon details of the relationship between you and your research partner that can increase the likelihood that you will get the timely, actionable information you need to make decisions. For example, you and the research may agree to:
 - Project kick-off, check-in and wrap-up meetings;
 - Deliverable formats (for example, reports; presentations/discussions with staff); and
 - Frequency of evaluation updates.

Additional Resources

DATA SHARING AND STUDENT PRIVACY

- The [DATA DRIVES School-Community Collaboration: Seven Principles of Effective Data Sharing](#) is a resource developed by StriveTogether and Data Quality Campaign that, in addition to outlining seven principles of data sharing, also provides links to case studies, sample documentation and additional data sharing resources.
- The [Ohio Department of Education Data Privacy Report](#) (2014) provides information about how federal and state law effect data collection, sharing and reporting at the state level. The report includes information about how the state approaches data privacy, data security and data sharing.
- The [National Center for Education Statistics \(NCES\) Forum Guide to Education Data Privacy \(2016\)](#) is a resource designed to help states and districts better understand the steps they can take to protect student privacy.
- The U.S. Department of Education's [Protecting Student Privacy](#) website provides a wide range of resources for education agencies interested in understanding FERPA regulations and the impact of those regulations on student data collection, sharing and reporting.

DATA SHARING FOR RESEARCH

- While targeted toward state education agencies, [the Data Quality Campaign's Roadmap for Effective Data Use and Research Partnerships between State Education Agencies and Education Researchers](#) includes many points relevant to districts as well.
- [The National Center for Education Statistics \(NCES\) Forum Guide to Supporting Data Access for Researchers: A Local Education Agency Perspective](#) provides best practices and templates for data sharing with researchers.
- [Research-Practice Partnerships: A Strategy for Leveraging Research for Educational Improvement in School Districts](#) outlines three major types of research practice partnerships and provides guidance on developing these partnerships.
- [The SEA of the Future: Building Agency Capacity for Evidence-Based Policymaking](#) is written with state agencies in mind but offers many insights into the importance of carrying out education research and evaluation.
- The [William T. Grant Foundation](#) has published a wide range of resources designed to educate districts, state education agencies and researchers on how to leverage research-practice partnerships.

OHIO DEPARTMENT OF EDUCATION DATA SHARING TEMPLATE

This template is being shared as a courtesy to local districts. Districts should consult their legal counsels about the proper use of this template prior to sharing any data with a third party for research and evaluation.

Memorandum of Understanding By and Between the Ohio Department of Education and _____

This agreement is entered into by the Ohio Department of Education (“Department”) and _____ (“Researcher”) for the purpose of sharing information between the parties in a manner consistent with the Family Educational Rights and Privacy Act of 1974 (“FERPA”). The information will be used by Researcher to conduct evaluative studies designed to improve instruction for children in the state of Ohio. Topics of these studies will include the following: _____. In order to complete these studies and in order to have a positive impact on the instruction of children, Researcher requires the use of student data from the Department.

The Family Educational Rights and Privacy Act (FERPA) describes circumstances under which State Educational Agencies (SEAs) are authorized to release data from an education record. This information can be disclosed to organizations conducting studies on behalf of SEAs, provided that federal, state or local law authorizes the evaluation in question. Ohio Revised Code §3301.12 grants to the Ohio state superintendent of public instruction the authority to conduct studies of education programs, but the provision prohibits the Department’s access to a student’s name, address or social security number.

- I. **PARTIES.** The Department is an SEA that is authorized to receive information from local educational agencies (“LEAs”) subject to FERPA, as authorized by 34 CFR Section 99.31. Researcher desires to conduct studies on behalf of the Department for the purpose of improving instruction in Ohio public schools in accordance with the Scope of Work Agreement attached hereto as Appendix A. The parties wish to share data collected by the Department regarding education in Ohio, none of which will allow the identification of individual students.
- II. **COMPLIANCE WITH LAW.** To affect the transfer of data subject to FERPA and other regulations, Researcher agrees to:
 1. In all respects comply with all applicable provisions of Ohio and federal laws, including FERPA. For purposes of this agreement, “FERPA” includes any amendments or other relevant provisions of federal law, as well as all requirements of Chapter 99 of Title 34 of the Code of Federal Regulations. 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 state or federal law or regulation.
 2. Use the data shared under this agreement for no purpose other than research authorized under Section 99.31(a)(3)(iv) or 99.31(a)(6) of Title 34 of the Code of Federal Regulations. Researcher further agrees not to share data received under this MOU with any other entity without the Department’s approval.
 3. Allow the Office of the State Auditor, subject to FERPA restrictions, access to data shared under this agreement and any relevant records of Researcher for purposes of completing authorized audits of the parties. Researcher shall be liable for any audit exception that results solely from its acts or omissions in the performance of this agreement. The Department shall be liable for any audit exception that results solely from its acts or omissions in the performance of this agreement. In the event that the audit exception results from the act or omissions of both parties, the financial liability for the audit exception shall be shared by the parties in proportion to their relative fault.
 4. Require all employees, contractors and agents of any kind to comply with all applicable provisions of FERPA and other federal laws with respect to the data shared under this agreement. Researcher agrees to require and maintain an appropriate confidentiality agreement from each employee, contractor or agent with access to data pursuant to this agreement. Nothing in this paragraph authorizes sharing data provided

under this agreement with any other entity for any purpose other than completing Researcher's work authorized under this agreement.

5. Maintain all data obtained pursuant to this agreement in a secure computer environment and not copy, reproduce or transmit data obtained pursuant to this agreement except as necessary to fulfill the purpose of the original request. Ensure that computing services operate at the moderate level baseline as defined in the National Institute of Standards and Technology (NIST) 800-53 Rev. 3 moderate baseline requirements and are consistent with Federal Information Security Management ACT (FISMA) requirements. All copies of data of any type, including any modifications or additions to data from any source that contains information regarding students, are subject to the provisions of this agreement in the same manner as the original data. The ability to access or maintain data under this agreement shall not under any circumstances transfer from Researcher to any other institution or entity.
6. Not to disclose any data obtained under this agreement in a manner that could identify an individual student to any other entity in published results of studies as authorized by this agreement. Not to provide any data obtained under this agreement to any party ineligible to receive data protected by FERPA or prohibited from receiving data from any entity. Contact the Department promptly in the event of a breach or potential breach of the security of, or loss of, student data. Such contact will be made to the Department's Chief Legal Counsel, Diane Lease (614-995-5927), and Chief Information Security Officer, Jason Mather (614-728-9014), or their successors. Researcher will cooperate and provide reasonable assistance to the ODE, at no charge, in the investigation of such breach or loss.
7. Notify the Department in advance of any new project or research question Researcher proposes to address and refrain from pursuing such changes without the Department's approval in the form of amendment to the MOU. Identify linkages of all data possessed by Researcher under this agreement and covered by FERPA to specific research studies and related publications.
8. Provide to the Department any materials designed for public dissemination, including presentations and embargoed report releases, based in whole or in part on data obtained under this agreement, at least 21 days prior to public release.
9. Destroy all data obtained under this agreement, within the time period indicated in Appendix A, when they are no longer needed for the purpose for which they were obtained. Nothing in this agreement authorizes Researcher to maintain data beyond the time period reasonably needed to complete the purpose of the request. All data no longer needed shall be destroyed or returned to the Department in compliance with 34 CFR Section 99.35(b)(2). Researcher agrees to require all employees, contractors or agents of any kind to comply with this provision.

III. UNAUTHORIZED DISCLOSURE AND INCIDENT REPORTING AND REMEDIATION AND PRIVACY AND SECURITY BREACH NOTIFICATION

1. Incident Reporting: Researcher shall immediately report to the Department's Chief Legal Counsel and Chief Information Security Officer the following:
 - a. Any use or disclosure of personal information which is not in compliance with the terms of this agreement or applicable law of which Researcher becomes aware; and
 - b. Any security incident of which Researcher becomes aware. For purposes of this agreement, "security incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
2. Within 24 hours of discovery of a suspected reportable incident as described in (1) above, Researcher shall notify the Department of the existence and nature of the incident as understood at that time. Researcher shall immediately investigate the incident and within 72 hours of discovery shall provide the Department, in writing, a report describing the results of Researcher's investigation, including:

- a. What data elements were involved, the extent of the data involved in the incident and, if applicable, the identification of affected individuals;
 - b. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed personal information or to have been responsible for the incident;
 - c. A description of where the personal information is believed to have been improperly transmitted, sent or utilized;
 - d. A description of the probable causes of the incident;
 - e. A description of the proposed plan for preventing similar future incidents, including ongoing risk remediation plan approval; and
 - f. Whether Researcher believes any federal or state laws requiring notifications to individuals are triggered.
3. Mitigation: Researcher agrees to mitigate, to the extent practicable, any harmful effect that is known to Researcher of a use or disclosure of personal information by Researcher in violation of the requirements of this agreement and report its mitigation activity back to the Department. Researcher shall preserve evidence.
 4. Coordination: Researcher will coordinate with the Department to determine additional specific actions that will be required of Researcher for mitigation of the incident, which may include notification to the individuals, entities or other authorities. Researcher will cooperate and provide reasonable assistance to the Department, at no charge, in the investigation of such breach or loss. Notifications, if any, will be made at the direction of the Department.
 5. Incident Costs: Researcher shall bear all actual and reasonably incurred costs associated with the incident that may be attributed solely to the negligent actions of Researcher. This may include, but not be limited to, costs associated with notifying affected individuals. It also may include the cost of investigation, remediation and assistance to individuals including services such as a standard level of credit-monitoring such as AllClear ID's standard service or other comparable service available to Ohio agencies under state term schedule. Researcher's obligation to cover these costs, as set forth above, is conditioned on Researcher receiving from the Department prompt written notice of any incident costs or claims and reasonable cooperation in its investigation and defense. Researcher may defend said claims at own expense with legal counsel of own choice. Notwithstanding the above, Researcher will not be required to cover any costs with respect to losses or expenses caused by the Department's own negligence or willful misconduct.

IV. DATA REQUESTS.

1. The Department may decline to comply with a request if it determines that providing the data in the manner requested would violate FERPA and/or would not be in the best interest of current or former students in Ohio public schools. All requests shall include a statement of the purpose for which data are requested and an estimation of the time needed to complete the project for which the data are requested. Data requests may be submitted by post, electronic mail or facsimile.
2. Researcher agrees that the Department makes no warranty concerning the accuracy of the student data provided.

- V. AUTHORIZED REPRESENTATIVE. Researcher shall designate in writing a single authorized representative able to request data under this agreement. The authorized representative shall be responsible for transmitting all data requests and maintaining a log or other record of all data requested and received pursuant to this agreement, including confirmation of the completion of any projects and the return or destruction data as required by this agreement. The Department or its agents may, upon request, review the records required to be kept under this section.

- VI. **RELATED PARTIES.** Researcher represents that it is authorized to bind to the terms of this contract, including confidentiality and destruction or return of student data, all related or associated institutions, individuals, employees or contractors who may have access to the data or may own, lease or control equipment or facilities of any kind where the data is stored, maintained or used in any way by Researcher. This agreement takes effect only upon acceptance by an authorized representative of Researcher, by which that institution agrees to abide by its terms and return or destroy all student data upon completion of the research for which they were intended or upon the termination of the Department’s current relationship with Researcher.

- VII. **TERM.** This agreement takes effect upon signature by an authorized representative of each party and will remain in effect until _____. The parties further understand that the Department may cancel this agreement at any time for reasonable cause, upon 30-day written notice. Notice of such cancellation shall be sent or otherwise delivered to the persons signing this agreement. The Department specifically reserves the right to immediately cancel this agreement upon discovery of noncompliance with any applicable federal or state laws, rules or regulations. Further, the Department specifically reserves the right to immediately cancel this agreement should the Department, in its sole discretion, determine that student information has been released in a manner inconsistent with this agreement, has not been maintained in a secure manner, or that substantially similar data access has become generally available for research purposes through any other mechanism approved by the Department. In the event of immediate cancellation, a notice specifying the reasons for cancellation shall be sent as soon as possible after the cancellation to the persons signing the agreement.

- VIII. **BREACH AND DEFAULT.** Upon breach or default of any of the provisions, obligations or duties embodied in this agreement, the parties may exercise any administrative, contractual, equitable or legal remedies available, without limitation. The waiver of any occurrence of breach or default is not a waiver of such subsequent occurrences, and the parties retain the right to exercise all remedies mentioned herein.

- IX. **AMENDMENT.** This agreement may be modified or amended provided that any such modification or amendment is in writing and is signed by the parties to this agreement. It is agreed, however, that any amendments to laws, rules or regulations cited herein will result in the correlative modification of this agreement, without the necessity for executing written amendment.

- X. **ASSIGNMENT OF RIGHTS.** Neither this agreement, nor any rights, duties or obligations described herein shall be assigned by Researcher without the prior express written consent of the Ohio Department of Education.

- XI. **ENTIRETY OF AGREEMENT.** All terms and conditions of this agreement are embodied herein and in the Scope of Work Agreement attached hereto as Appendix A. No other terms and conditions will be considered a part of this agreement unless expressly agreed upon in writing and signed by both parties.

 Paolo DeMaria
 Superintendent of Public Instruction

 Date

 Heather Boughton
 Director, Office of Research, Evaluation and Advanced Analytics

 Date

 [Printed Name – authorized signatory for agreement]
 [Title]
 [Name of Organization]

 Date

Ohio Department of Education
Memorandum of Understanding Template
Appendix A: Scope of Work Agreement

I. Scope of Work

Provide a brief description of the research study for which the researcher is requesting data per this data sharing agreement. Include a description of the research questions being addressed, as well as a description of any reports expected to be generated as a result of this research study. Note that Ohio’s MOU (Section II.7) requires the researcher to provide the Ohio Department of Education with annual updates on the research study or studies for which the data shared per this agreement is being used.

A more detailed description of the research method, internal quality and security assurances, and research context or justification may be submitted alongside the draft MOU.

II. Estimated Project Timeline

Provide a brief description of the estimated timeline for the research study supported by this MOU. Note that Ohio’s Memorandum of Understanding (Section VII) requires the researcher to identify an effective end date for the MOU. Include in this description the estimated time frame needed to destroy or return the data in accordance with the MOU (Section 11.8). Any extensions to the effective end date or the time frame for destruction or return of the data will require a signed addendum to the original MOU.

III. Authorized Representative

Ohio’s Memorandum of Understanding (Section V) requires the researcher to designate in writing a single authorized representative responsible for transmitting all data requests and maintaining a log or other record of all data requested and received pursuant to this agreement, including confirmation of the completion of any projects and the return or destruction of data as required by this agreement.

[Printed Name – authorized representative for data transactions]

[Title]

[Name of Organization]

[Physical Address]

[Phone Number]

[Email Address]

IV. Description of Data Being Requested

Provide a detailed description of the data elements requested per this data sharing agreement. Include in your description information about the years of data being requested, the educational entities for which you would like data (all schools, specific schools, specific types of schools, etc.) and the specific data elements being requested for this research study.

V. Communication

In collaboration with the Department, develop and provide a description of any agreed-upon expectations, norms, formats or deliverables related to ongoing communications between the Department and the researcher. For example, include agreed-upon expectations regarding kick-off, interim, and wrap-up meetings, deliverable formats and/or frequency of updates.

DATA SHARING TEMPLATES: CONSIDERATIONS FOR DISTRICTS PARTICIPATING IN SCHOOL-BASED HEALTH CARE

The Ohio Department of Education's standard data sharing template solely focuses on sharing educational records. Districts that are engaged in school-based health care initiatives and intend to share data with a third party for program evaluation of those initiatives also will want to consult with their legal counsels to better understand how to appropriately address Health Insurance Portability and Accountability Act-related (HIPAA) regulations.

Sample language that districts may want to consider adding to data sharing agreements designed to support program evaluation of school-based health care programs may include:

Confidentiality and the Health Insurance Portability and Accountability Act

- a. Provider and District shall comply with all applicable provisions of Ohio and federal laws including the Health Insurance Portability and Accountability Act (hereinafter "HIPAA") or its state equivalent. HIPAA includes any amendments or other relevant provisions of federal law, as well as all requirements of Chapters 160 through 164 of Title 45 of the Code of Federal Regulations. Nothing in this Agreement shall be construed to allow either party to maintain, use, disclose, or share protected health information ("PHI") in a manner not allowed by either state or federal laws or regulations.
- b. As used herein, PHI means individually identifiable information including but not limited to the past, present or future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual, as more fully defined under 45 CFR 164.501 and any amendments thereto.
- c. Each party shall use PHI only for the terms of this Agreement as set forth herein. Each party agrees to use reasonable efforts to safeguard PHI and shall conform with the Privacy and Security requirements under 45 CFR 165 and 45 CFR 164 to protect the data.
- d. If Provider experiences any breach of data security that exposes confidential information, that party shall bear all costs to notify every individual whose confidential information may have been compromised.