

Data-Sharing Agreements: A Technical Introduction

This introduction provides foundational information about how to set up a data-sharing agreement that enables the sharing of individual-level student records. First, it provides an overview of federal laws that govern the transfer and use of personally identifiable information (PII). Then, it discusses the essential components of a data-sharing agreement. Finally, it gives a high-level summary of data governance practices for transferring, storing, and using student data. Please scroll to the bottom to see a list of related online resources.

Federal privacy laws

Family Education Rights Privacy Act (FERPA) protects the privacy of student education records.

Who is covered? Students in all schools and colleges that receive funds from the U.S. Department of Education. Information about parents and families is also protected. Parents have rights over most educational records until students turn 18 or attend a postsecondary institution.

What are the most common exceptions to parental and student consent? Parents or adult students must give consent for their data to be accessed and used, with a few exceptions¹:

Key terms:

Family Education Rights Privacy Act (FERPA): Primary federal law governing the protection of information about student and family education records.

Institutional Review Board (IRB): A formal committee that reviews all research involving human participants to protect their rights and welfare.²

Personally identifiable information (PII): Information that can be used to identify an individual, either alone or in combination with other identifying information, such as demographic or location data³.

1. *Studies exception.* This exception allows organizations to conduct studies for or on behalf of schools, districts, or postsecondary institutions for the purpose of improving instruction.
2. *Audit or evaluation exception.* This exception is for organizations to evaluate federal- or state-supported education programs or to conduct an audit, evaluation, or compliance activity as required by federal regulations.
3. *Building capacity.* This exception is for consultants who are performing a service or function that the data provider would normally use their own employees for.

¹ Source: U.S. Department of Education. (n.d.) The family educational rights privacy act: Guidance for reasonable methods and written agreements. https://www2.ed.gov/policy/gen/guid/fpco/pdf/reasonablemtd_agreement.pdf

² Source: U.S. Food and Drug Administration. (1998). Institutional Review Boards Frequently Asked Questions: Guidance for Institutional Review Boards and Clinical Investigators. <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/institutional-review-boards-frequently-asked-questions>

³ Source: U.S. General Services Administration. (2019). Rules and Policies – Protecting PII – Privacy Act <https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act>

Health Insurance Portability & Accountability Act (HIPAA)

Health and Human Services departments typically manage foster care and homelessness records, and less commonly needed for education studies or reporting medical records related to education outcomes. To obtain individual health care records, the project must be approved by an institutional review board (IRB) and satisfy three criteria⁴:

1. There must be no more than *minimal risk* to the privacy of individuals and a plan to protect identifiers from improper disclosure, destroy identifiers as soon as they are no longer necessary, and assurances that the information will not be reused or disclosed
2. It is not feasible to conduct the research without the waiver
3. It is not possible to conduct the research without access to protected health information

Establishing data-sharing agreements

A data-sharing agreement is a signed agreement between two or more entities that establishes the manner in which data will be transferred, stored, used, and destroyed according to local requirements and state and federal laws.

According to the FERPA, the following elements must be included in any agreement to establish the transfer and storage of students' PII:

- *Purpose*. The purpose of the agreement should state the project goals and expected benefits to students, educators, communities, or other groups. It should identify the funding organization(s) and the names of the organizations the project is intended to support. State which FERPA exception applies to the project.
- *Scope*. The scope should describe the proposed work using the data and, where applicable, statistical methods for analysis, how results will be reported as well as to whom. A justification for requesting PII should be included.
- *Duration*. State the start and end dates for the term that the data are needed to fulfill the purpose and scope of the project, as well as potential audits or other needs relevant to the named project. Describe the means for disposition of the data at the end of the term.
- *Information to be disclosed*. Provide categories of data with examples of specific fields, as well as other parameters such as years of data being requested. Other data sources that will or may be combined with the requested data should be indicated. Provide tables that display each data element and the way it will be used.
- *Formally authorized representative*. Identify an individual or organization to be responsible for ensuring the terms of the agreement are met and as a point of contact for the data provider.
- *Statements of data security and confidentiality*. Explain how all parties will protect PII, including the processes and systems in place to protect data during transfer, storage,

⁴ Department of Health and Human Services. (2017). OCR HIPAA Privacy: Research. <https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html>

and use. This may include required training and background checks for people who access the data, periodic audits, cyber insurance, and institutional review board approval for the project.

Data governance for long-term cross-agency projects

Long-term and ongoing projects that use data from several agencies require cooperation and commitment among all partners who will share or use data for the project. Some key actions partners seeking to build a cross-agency data system need to take include:

- *Agreeing to participate.* Establish a memoranda of understanding (MOU) signed by each partner that will contribute data to the project. The MOU should ensure compliance with federal, state, and local privacy laws and facilitate regular data updates without having to go through a lengthy procurement process each year.
- *Electing a partner to house the data.* One partner or an external contractor will need to collect and house data from each partner. The hosting partner must have sufficient technological and human capacity to secure, link, and analyze the data.
- *Establishing policies and procedures.* These include, but are not limited to, defining a decision-making process among the partners, documenting data security and risk management systems, identifying the data elements to be stored and how they will be processed to ensure quality, and disclosing how data will be accessed and by whom.
- *Regularly reviewing the process.* Select a committee with representatives from each partner to regularly review and update MOUs, policies, and procedures. Arrange for periodic audits to ensure adherence to procedures and policies.

Resources

General resources

- U.S. Department of Education Privacy Technical Assistance Center
<https://studentprivacy.ed.gov/>
- U.S. General Services Administration. (2019). Rules and Policies – Protecting PII – Privacy Act <https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act>
- CITI Research Ethics and Compliance Training (fees apply for certification)
<https://about.citiprogram.org/en/series/irb-administration/>

Federal Privacy Laws and Institutional Review Boards

- U.S. Department of Education. (n.d.). The family educational rights privacy act: Guidance for reasonable methods and written agreements.
https://www2.ed.gov/policy/gen/guid/fpco/pdf/reasonablemtd_agreement.pdf

- U.S. Department of Education Privacy Technical Assistance Center. (n.d.) Online training modules about FERPA and data-sharing agreements
<https://studentprivacy.ed.gov/content/online-training-modules>
- Department of Health and Human Services. (2017). OCR HIPAA Privacy: Research. Explanation of how HIPAA applies to research. <https://www.hhs.gov/hipaa/for-professionals/special-topics/research/index.html>
- U.S. Department of Health and Human Services. (2018). Institutional Review Board Written Procedures: Guidance for Institutions and IRBs.
<https://www.hhs.gov/ohrp/regulations-and-policy/guidance/institutional-issues/institutional-review-board-written-procedures/index.html>
- U.S. Food and Drug Administration. (1998). Institutional Review Boards Frequently Asked Questions: Guidance for Institutional Review Boards and Clinical Investigators.
<https://www.fda.gov/regulatory-information/search-fda-guidance-documents/institutional-review-boards-frequently-asked-questions>
- U.S. Department of Health and Human Services. (2016). Basic decision trees for IRB determination from the department. <https://www.hhs.gov/ohrp/regulations-and-policy/decision-charts/index.html>

Data-sharing Agreements

- U.S. Department of Education Privacy Technical Assistance Center. (2012). Written agreement checklist. Summarizes elements required for data-sharing agreements under the FERPA exceptions for studies or audits and or evaluations.
https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Written_Agreement_Checklist.pdf
- U.S. Department of Education Privacy Technical Assistance Center. (2015). The Family Educational Rights Privacy Act: Guidance for reasonable methods and written agreements.
https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Guidance_for_Reasonable_Methods%20final_0.pdf
- U.S. Department of Education Institute of Education Sciences. Guiding principles for successful data-sharing agreements. (2019).
<https://ies.ed.gov/blogs/research/post/guiding-principles-for-successful-data-sharing-agreements>

Data governance for long-term cross-agency projects

- U.S. Department of Education Privacy Technical Assistance Center. (2017). Integrated data systems and student privacy. Provides guidance on how to protect personally identifiable information and comply with state and federal laws when developing and using cross-agency longitudinal data systems.
https://studentprivacy.ed.gov/sites/default/files/resource_document/file/IDS-Final_0.pdf

- U.S. Department of Education Privacy Technical Assistance Center. (2011). Data governance checklist. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Data%20Governance%20Checklist_0.pdf
- U.S. Department of Education Institute of Education Sciences. (2014). State Longitudinal Data Systems P-20+ Best Practices. https://nces.ed.gov/programs/slds/pdf/P-20W_Best_Practices.pdf