



NATIONAL RESEARCH STUDENT DATA PRIVACY AGREEMENT GUIDANCE

Version: 1.0

© 2021 Access 4 Learning (A4L) Community. All Rights Reserved.

This document may only be used by A4L Community members and may not be altered in any substantive manner.

Usage Guidance

FERPA Studies Exception

https://studentprivacy.ed.gov/sites/default/files/resource_document/file/Written_Agreement_Checklist_0.pdf

PTAC-CL-3, April 2012 (revised July 2015) 1

This ***National Research Data Privacy Agreement*** (NRDPA) leverages the successful [National Data Privacy Agreement](#) (NDPA) developed by the [Student Data Privacy Consortium](#) (SDPC) that is in use in thousands of data privacy agreements between end users and suppliers to address the School Business Official exception within the Family Educational Rights and Privacy Act (FERPA). The FERPA ***research studies exception*** allows for the disclosure without consent of existing personally identifiable information (PII) from education records to organizations conducting studies “for, or on behalf of,” educational agencies or institutions. These studies can only be for the purpose of developing, validating, or administering predictive tests; administering student aid programs; or improving instruction. **This NRDPA is NOT for FERPA’s audit or evaluation exceptions. The NRDPA is specifically designed to standardize the various required components for the studies exception with the focus on existing data usage.**

Under the studies exception, written agreements must:

- Specify the following elements:
 - Purpose of the study to be conducted
 - Scope of the proposed study
 - Duration of the study, and
 - Information to be disclosed
- Require the organization to:
 - Use PII from education records only to meet the purpose(s) of the study
 - Limit access to PII to those with legitimate interests
 - Conduct the study in a manner that doesn’t permit the identification of parents or students by anyone other than representatives of the organization with legitimate interests, and
 - Destroy all PII when the information is no longer needed for the purposes for which the study was conducted and within a specified time period.

Please see 34 CFR §99.31(a)(6) for more information

In addition to the absolute minimum mandatory requirements, there are a number of best practices that organizations should consider when entering into written agreements. (For details, see [PTAC's Guidance for Reasonable Methods and Written Agreements](#), specifically the content that deals with the studies exception.)

Disclosing entities are encouraged to examine the list provided below and tailor the practices as necessary and appropriate to their specific circumstances:

- Bind individuals to the agreement
- Agree on limitations on use of the PII, including any methodological restrictions, such as linking to other datasets.
- Specify points of contact and data custodians
- Mention Institutional Review Board review and approval.
- State ownership of PII.
- Identify penalties for inappropriate disclosure
- Set terms for data destruction.
- Include funding terms.
- Maintain the right to audit.
- Identify and comply with all applicable legal requirements, including maintaining the data in a secure manner by applying appropriate technical, physical, and administrative safeguards to properly protect the PII, both at rest and in transit.
- Have plans that are in accordance with any applicable state and Federal laws for responding to a data breach, including, when appropriate or required, responsibilities and procedures for notification and mitigation.
- Review and approve reported results
- Define terms for conflict resolution
- Specify modification and termination procedures, including approved destruction methods for each specific type of media (e.g., data wiping, degaussing, shredding, etc.)
- Inform the public about written agreements

Note: Parties are encouraged to review and redact, prior to publication, any data security provisions that may aid those seeking unauthorized access to systems. In some cases, a separate confidential IT Security Plan may be appropriate.