Privacy Impact Assessment (PIA)

for the

National Center for Education Statistics (NCES) Applications at RTI

April 4, 2022

For PIA Certification Updates Only: This PIA was reviewed on **Enter date** by **Name of reviewer** certifying the information contained here is valid and up to date.

Contact Point

Contact Person/Title: Gail Mulligan, Longitudinal Surveys Branch Chief
Contact Email: Gail.Mulligan@ed.gov

System Owner

Name/Title: Tracy Hunt-White, System Owner
Principal Office: Institute of Education Sciences (IES)

Please submit completed Privacy Impact Assessments to the Privacy Office at privacysafeguards@ed.gov

*Please complete this **Privacy Impact Assessment (PIA)** on how personally identifiable information (PII) is collected, stored, protected, shared, and managed electronically by your system. You may wish to consult with your ISSO in completing this document.*
If a question does not apply to your system, please answer with N/A.

1. Introduction

1.1. Describe the system including the name, acronym, and a brief description of the program or purpose for the system.

National Center for Education Statistics Applications at RTI (NCES Applications at RTI) is a U.S. Department of Education (Department) system that includes Institute of Education Sciences (IES) projects performed by RTI International (RTI). RTI is a contractor for several NCES studies. RTI is a U.S.-based nonprofit research organization. NCES Applications at RTI is an IT system hosted at RTI.

IES conducts many studies to understand the condition of education in the United States. The NCES Applications at RTI system processes data collected by IES/NCES studies (through web surveys, telephone interviews, in-school data collection, and administrative record matching) and prepares the data for public dissemination on the IES websites hosted in the IES Data Center (IESDC). NCES Applications at RTI currently consist of the following IES projects:

- National Postsecondary Student Aid Study (NPSAS)
- High School Longitudinal Study of 2009 (HSLS:09)
- Baccalaureate and Beyond Longitudinal Study (B&B)
- Beginning Postsecondary Students Longitudinal Study (BPS)
- National Longitudinal Transition Study 2012 (NLTS 2012)
- Middle Grades Longitudinal Study of 2017-18 (MGLS:2017)
- High School and Beyond Longitudinal Study of 2022 Study (HS&B:22)

NCES Applications at RTI processes and analyzes survey and assessment data collected by NCES and administrative data obtained through records matching. Survey data consist of responses from students, their parents or legal guardians, teachers, administrators, service providers (e.g., school staff who provide additional individual-level assistance outside of main classroom or special education providers, e.g., speech language therapists, occupational therapists, etc.), and other adults to data collection instruments including information about background and demographic data, family characteristics, education and/or employment experiences, finances, aspirations, plans, and attitudes. Assessments developed by NCES are administered in the middle and secondary longitudinal studies. Cognitive assessment scores, administrative and

financial aid records, and high school and college transcripts are also appended to the records. Administrative data are obtained from data sources such as Federal Student Aid's National Student Loan Data System (NSLDS) and Central Processing System (CPS). In addition, data are obtained from external sources such as the National Student Clearinghouse (NSC), ACT, College Board, and the Veterans Benefits Administration. PII is used to match individuals sampled for the NCES surveys to their administrative record in these data sources.

Survey data from NCES and other data sources go through data processing. Data processing includes editing the data, applying confidentiality protocols such as perturbation,[1] deriving variables that will be used for data analysis, conducting imputation,[2] and weight adjustments to create a final de-identified data set. This data set is used to generate estimates and reports that are published by NCES. RTI delivers to NCES this final de-identified data set in which all direct identifiers are removed. Data are subjected to perturbation procedures to minimize disclosure risk and protect the confidentiality of information about specific individuals. This minimizes the risk that an individual respondent in a data file could be identified.

1.2. Describe the purpose for which the personally identifiable information (PII)[3] is collected, used, maintained or shared.

This system is used to fulfill NCES's statutory mandate to collect, report, analyze, and disseminate statistical data on the condition and progress of education in the United States and other nations at the early childhood, preschool, elementary, secondary, postsecondary, and adult levels. PII is collected by IES/NCES in order to help meet this mandate. The NCES Applications at RTI system processes data collected by IES/NCES survey collections and prepares the data for public dissemination on the IES websites. Direct identifiers are needed to sample institutions and students, to collect information from institutions and students, and to conduct records matching that allows for the collection of information about study members from administrative records. In addition, for some studies, locating information (e.g., student/respondent name, home address, telephone number, email) must be collected in order to track study members over time so that they can be contacted for follow-up data collections. Without this information,

[1] Data perturbation is a data security technique that adds "noise" to databases to allow individual record confidentiality.
[2] Imputation preserves all cases by replacing missing data with an estimated value based on other available information. Once all missing values have been imputed, the data set can then be analyzed using standard techniques for complete data.
[3] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. OMB Circular A-130, page 33

contacting and retaining respondents at each data collection round would be extremely difficult.

1.3. Is this a new system, or one that is currently in operation?

Currently Operating System

1.4. Is this PIA new, or is it updating a previous version?

Updated PIA

The PIA is being updated as part of the required biennial review.

1.5. Is the system operated by the agency or by a contractor?

Contractor

1.5.1. If the system is operated by a contractor, does the contract or other acquisition-related documents include privacy requirements?

☐ N/A

Yes

2. Legal Authorities and Other Requirements

If you are unsure of your legal authority, please contact your program attorney.

2.1. What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system? Please include name and citation of the authority.

NCES is authorized by law to collect and use these data under the Education Sciences Reform Act of 2002 (ESRA) (20 U.S. Code Section 9543): "The Statistics Center shall collect, report, analyze, and disseminate statistical data related to education in the United States and in other nations, including — (7) conducting longitudinal and special data collections necessary to report on the condition and progress of education." In addition, the National Postsecondary Student Aid Study (NPSAS) and its related longitudinal studies, the Beginning Postsecondary Students Longitudinal Study, and the Baccalaureate and Beyond Longitudinal Study are also covered by the Higher Education Opportunity Act of 2008 [HEOA 2008, 20 U.S.C. §1015(a)(k)].

SORN

2.2. Is the information in this system retrieved by an individual's name or personal identifier such as a Social Security Number or other identification?

Yes

Information is retrieved by an individual's name, date of birth, and social security number.

2.2.1. If the above answer is **YES,** this system will need to be covered by Privacy Act System of Records Notice(s) (SORN(s)).[4] Please provide the SORN name, number, Federal Register citation and link, or indicate that a SORN is in progress.

☐ N/A

The NCES SORN, entitled the "National Center for Education Statistics Longitudinal Studies and the School and Staffing Surveys" (18-13-01), 83 FR 56831, was published in the Federal Register on November 14, 2018.

2.2.2. If the above answer is **NO**, explain why a SORN was not necessary. For example, the information is not retrieved by an identifier, the information is not maintained in a system of records, or the information is not maintained by the Department, etc.

☑ N/A

Records Management
If you do not know your records schedule, please consult with your records liaison or send an email to RMHelp@ed.gov

2.3. What is the records retention schedule approved by National Archives and Records Administration (NARA) for the records contained in this system? Please provide all relevant NARA schedule numbers and disposition instructions.

IES is waiting on the 21st Century Information Retention Policy Framework to be approved and implemented. In that Framework, NCES studies would fall under DAA-0441-2021-0002-0003 II.A. Completed Research and Statistical Studies.

[4] A System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by ED. https://connected.ed.gov/om/Documents/SORN-Process.pdf

Until that framework is implemented, the records will not be destroyed until such time as NARA approves said schedule.

2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timelines in the records disposition schedule?

Yes

3. Characterization and Use of Information

Collection

3.1. List the specific PII elements (e.g., name, email, address, phone number, date of birth, Social Security, etc.) that the system collects, uses, disseminates, or maintains.

The PII stored within the NCES Apps at RTI system varies depending on the study. If the student is in a study for elementary or secondary students, PII consists of data such as name, physical address, phone number, Social Security number (SSN), date of birth, email address, financial information, schools attended, educational information, disability and/or exclusion status, student/school ID, employment information, parent name, and parent address.

This system also contains responses from students, their parents or legal guardians, teachers, administrators, counselors, and other adults to data collection instruments. The specific information collected varies by study but includes information such as background and demographic data, functional measures (reports of children's functioning in cognitive, social, emotional, and physical domains), family characteristics, education and/or employment experiences, finances, aspirations, plans, and attitudes. Assessments developed by NCES are administered in the middle and secondary longitudinal studies. Cognitive assessment scores, administrative records, and high school transcripts are also appended to some records. The appended administrative records contain data such as attendance, program participation, and other information.

For postsecondary studies, PII stored consists of items such as contact information for students and parents: names, addresses, telephone numbers, and email addresses. Information specific to the student include data such as student's SSN, date of birth, race/ethnicity, sex/gender, disability status, income, institution attended, financial aid and enrollment information, major, and degree data. Also, administrative records and postsecondary education transcripts are appended to some records. The appended administrative records contain data such as admissions test scores, veterans' benefits information, and courses taken and grades.

The records for schools/institutions contain information such as numbers and characteristics of students, teaching staff, and administrators; data on facilities, programs, services, school climate, discipline and safety, technology; and information related to student admissions, enrollment, and performance. The records related to teachers and administrators contain data on topics such as certifications, training, experience, coursework, technology usage, and attitudes and opinions related to various aspects of education and operations.

3.2. Does the system collect only the minimum amount required to achieve the purpose stated in Question 1.2?

Yes

IES/NCES collects only the minimum information necessary. The NCES Applications at RTI system processes data collected by IES/NCES survey collections and prepares the data for public dissemination on the IES websites. Direct identifiers, as authorized by the ESRA, are needed to sample institutions and students, to conduct record matching that allows for the collection of information about study members from administrative records and, for longitudinal studies, to follow study participants over time. The use of direct identifiers is minimized to the fullest extent possible and are kept secure within the network at RTI.

3.3. What are the sources of PII collected (e.g., individual, school, another agency, commercial sources, etc.)?

Educational institutions, students, parents or legal guardians, teachers, administrators, and service providers.

3.4. How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, web page, database, etc.)?

NCES maintains a website (nces.ed.gov/surveys) that is used to collect the information from institutions and individuals. In addition, for in-school data collections, the data are collected on laptops, stored, encrypted and transferred to NCES Apps at RTI. The NCES Applications at RTI system is not used to directly collect respondent data, but to process and analyze survey data collected by NCES and administrative data obtained through record matching.

3.5. How is the PII validated or confirmed to ensure the integrity of the information collected?[5] Is there a frequency at which there are continuous checks to ensure the PII remains valid and accurate?

NCES maintains the website (nces.ed.gov/surveys) that is used to collect the information from institutions and individuals. The NCES Applications at RTI are not used to directly collect respondent data. For individuals, there are edit checks built into the survey instrument. For example, logic in the code used to develop the surveys prevent reporting of erroneous information (e.g., prevents access to questions about spouse's education when the respondent reports being "single, never married"). Additionally, edit checks are built into the survey instrument to validate values that are extreme and/or out of range. For institutions, there are similar edit checks built in their data collection instrument. Once data are collected and reviewed, the data provider may contact respondents to address questions about the data. In addition, the data undergo extensive quality checks before official statistics are produced and published.

Use

3.6. Describe how the PII is used to achieve the purpose stated in Question 1.2 above.

RTI maintains project data for use conducting longitudinal studies (e.g., to be able to follow study respondents as they complete high school and transition to the work force or postsecondary education or to follow study respondents as they transition from the completion of a baccalaureate program into the work force or additional higher education). De-identified data, which contain no direct identifiers and are perturbed to minimize the risk that individual respondents can be identified, are delivered from RTI to the IES Data Center (IESDC) system to build data tools and generate tables and reports on various topics. The data tools and reports are made public, accessible on the NCES website. In addition, a restricted-use micro-level data file (which contains no direct identifiers and is perturbed for disclosure avoidance to minimize the risk that individual respondents can be identified) is made available to researchers who obtain a restricted-use[6] data license. In order to qualify for a license, researchers must have a legitimate research question that can only be answered with restricted-use data, must meet requirements to assure the security of the data, and must sign a notarized agreement that they will abide by the license requirements or face penalties for misuse of the data. Information about the restricted-use license process can be found at: https://nces.ed.gov/statprog/instruct.asp.

[5] Examples include restricted form filling, account verification, editing and validating information as it's collected, and communication with the individual whose information it is.

[6] Federal agencies collect survey data containing individually identifiable information that are confidential and protected by law. This information is not publicly released. The terms "restricted-use data" and "subject data" are used to refer to data of this type.

3.7. Is the system using PII for testing/researching new applications or information systems prior to deployment or for training employees?

No

3.7.1. If the above answer is **YES,** what controls are in place to minimize the risk and protect the data?

☑ N/A

Social Security Numbers

It is the Department's Policy that, in order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.

3.8. Does the system collect Social Security Numbers? Note that if the system maintains Social Security Numbers but does not explicitly collect them, answer 3.8.1 to address the purpose for maintaining them.

Yes

3.8.1. If the above answer is **YES**, explain the purpose for its collection, and how the SSN will be used.

☐ N/A

SSNs are collected for the purpose of record matching with Department systems and other administrative databases, such as the NSC, which provides enrollment data for the members of the sample. For longitudinal studies, the SSN may also be used for tracking study respondents as they change schools and/or geographic locations over the course of the study (e.g., to be able to follow study respondents as they complete high school and transition to the work force or postsecondary education or to follow study respondents as they transition from the completion of a baccalaureate program into the work force or additional higher education). NCES keeps abreast of studies that focus on the use of names for such linkages and follow-up studies, but the return rate on matches based only on name is substantially lower than that obtained using SSN. SSNs are never publicly disclosed.

3.8.2. Specify any alternatives considered in the collection of SSNs and why the alternatives were not selected.

☐ N/A

NCES keeps abreast of studies that focus on the use of names for such linkages and follow-up studies, but the return rate on matches based only on name is substantially lower than that obtained using SSN. The likelihood of successful matches absent the SSN is much lower; missing data reduce overall data quality.

4. Notice

4.1. How does the system provide individuals with notice about the collection of PII prior to its collection (e.g., direct notice, such as a Privacy Act Statement (if applicable) or public notice, such as a SORN, PIA)? If notice is not provided, explain why not.

In the case of surveys conducted in educational institutions, advance letters are sent to the administrator of the institution describing the study, explaining the voluntary nature of the study, and describing the pledge of data confidentiality. In addition, every IES data collection that includes PII also includes a Privacy Act Statement, description of the voluntary nature of the data collection and a pledge of confidentiality, per OMB standards and NCES Statistical Standard 4.2.

The text of the pledge of confidentiality includes the following: Your answers may be used only for statistical or research purposes and may not be disclosed, or used, in identifiable form for any other purpose except as required by law.

Furthermore, the routine statistical purposes for which the data may be used must be explained. If an individual educational institution requires informed consent from parents or adult students, that is included in the data collection procedures, otherwise each respondent is informed of the voluntary nature of their participation as it applies to both the entire data collection and to individual questions within the data collection. If the institutional data include data that are potentially disclosive of individual characteristics IES uses professional best practices to protect the identity of individuals in an institution when publishing data from the collection.

4.2. Provide the text of the notice or the link to the webpage where the notice is posted if notice is provided other than by SORN or PIA.

☐ N/A

The notice is tailored to specific respondent types and will vary by study. For an example of the notices, please see the student data collection website for the 2020/22 Beginning Postsecondary Students Longitudinal Study.

4.3. What opportunities are available for individuals to consent to uses (including new uses of previously collected PII), decline to provide PII, or opt out of the project?

When respondent data are collected by applications at NCES, adult respondents are assured of the confidential nature of the data collection and are asked to provide informed consent prior to the start of data collection. The informed consent statement is built into the data collection instrument. It is one of the initial screens that respondents encounter before answering questions. Adult respondents must give their consent before being asked the first question. Parents/guardians provide consent for their children to participate in the middle and secondary longitudinal studies. All individuals, both minors and adults, may decline to participate in the study, and they may opt out of a **s**tudy at any time after providing initial consent by contacting NCES and/or the data collection contractor. They may also decide not to provide any type of response to a solicitation for information. In addition, if an individual does choose to participate in a study, he or she is also free to decline to answer any question at any time.

4.4. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practice, policy, or activities that affect the PII and privacy to ensure that individuals are aware of and can consent to, where feasible, these changes?

Yes

5. Information Sharing and Disclosures

Internal

5.1. Will PII be shared internally with other ED principal offices? If the answer is **NO**, please skip to Question 5.4.

Yes

5.2. What PII will be shared and with whom?

☐ N/A

RTI performs record matching with the Department's FSA NSLDS and the CPS. Record matching is conducted using SSNs, last name, and date of birth. Data are transmitted

from the RTI to FSA for purposes of the matching by using a Secure Sockets Layer (SSL) encrypted website provided by FSA.

5.3. What is the purpose for sharing the specified PII with the specified internal organizations?

☐ N/A

Record matching is performed with CPS to obtain data on demographic characteristics about respondents, to include their dependency status and expected family contribution, and to obtain NSLDS data on amount and types of Federal aid received.

External

5.4. Will the PII contained in the system be shared with external entities (e.g. another agency, school district, the public, etc.)? If the answer is **NO**, please skip to Question 6.1.

Yes

5.5. What PII will be shared and with whom? List programmatic disclosures only.[7]
Note: If you are sharing Social Security Numbers externally, please specify to whom and for what purpose.

☐ N/A

PII is collected first from institutions to identify the study sample. When available, this information includes SSN. Additional PII, including SSN if not already obtained, will be collected from sample members during the survey/interview. PII collected will be shared with external sources to assist with locating sample members (e.g., LexisNexis, National Change of Address) and with administrative data sources, including Federal (e.g., Veterans Benefits Administration) and nonfederal (e.g., NSC, SAT, ACT, College Board) sources. There are approved sharing agreements in place to conduct matching with any external data sources and all individuals involved in the matching process must sign an Affidavit of Nondisclosure or adhere to another type of legally enforceable confidentiality agreement.

5.6. What is the purpose for sharing the PII with the specified external entities?

☐ N/A

[7] If this information is covered by Privacy Act System of Records Notice (SORN) please list only relevant programmatic disclosures listed under the Routine Uses section.

Record matching with these sources is conducted to obtain information on students' enrollment history and degree completion, college admissions test scores, and information on the attendance status, credit hours, majors, State and institutional financial aid, and veterans' educational benefits. In addition, PII is shared with the sources listed above to locate sample members not otherwise located by way of provided address and telephone information.

5.7. Is the sharing with the external entities authorized?

☐ N/A

Yes

5.8. Is the system able to provide and retain an account of any disclosures made and make it available upon request?

☐ N/A

Yes

The record of disclosure(s) are maintained within a file share folder structure that indicates the vendor/matching company, the date, the data sent, and the data received. The folder structure is maintained throughout the course of the contract and archived with the rest of the project when the project ends. A record of disclosures can be made available upon request.

5.9. How is the PII shared with the external entity (e.g. email, computer match, encrypted line, etc.)?

☐ N/A

IES has a secure data transfer system, which uses SSL technology, allowing the transfer of encrypted data over the Internet. The IES File Transfer System is used for all administrative data sources that do not have their own secure file transfer system. For example, matching to NSLDS uses EdConnect, which provides secure transfer protocol. NSC uses PGP encryption and transfer occurs via their secure website. In all cases, data transfers are encrypted and sent securely via Secure Shell (SSH) File Transfer Protocol (sFTP).

5.10. Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

☐ N/A

Yes

5.11. Does the project place limitation on re-disclosure?

☐ N/A

Yes

6. Redress

6.1. What are the procedures that allow individuals to access their own information?

If an individual wishes to access the content of a record in this system of records, they should contact the system manager with necessary particulars such as the study in question, name, current address, the date and place of birth, and any other identifying information requested by the Department, while processing the request, to distinguish between individuals with the same name. The individual must meet the requirements in 34 CFR 5b.5, including proof of identity.

6.2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

If an individual wishes to contest the content of a record in this system of records, they should contact the system manager with necessary particulars such as the study in question, name, current address, the date and place of birth, and any other identifying information requested by the Department, while processing the request, to distinguish between individuals with the same name, identify the specific items to be changed; and provide a written justification for the change. Requests to amend a record must meet the requirements of the regulations in 34 CFR 5b.7.

6.3. How does the project notify individuals about the procedures for correcting their information?

The system of records notice listed in question 2.2 explains the procedures for correcting customer information.

7. Safeguards

If you are unsure which safeguards will apply, please consult with your ISSO.

7.1. Does the principal office work with their CSO/ISSO to build privacy & security into the system and build privacy extensions to the extent feasible?

Yes

7.2. Is an Authority to Operate (ATO) required?

Yes

7.3. Under NIST FIPS Pub. 199, what is the security categorization of the system: **Low, Moderate, or High?**

☐ N/A

Moderate

7.4. What administrative, technical, and physical safeguards are in place to protect the information?

Access to the records is limited to authorized personnel who are briefed regarding confidentiality of the data, are required to sign a written statement attesting to their understanding of the significance of the confidentiality requirement and penalties for non-compliance and have received Department security clearances. Security systems limit data access to contract staff on a "need to know" basis and control each individual user's ability to access and alter records within the system. The NCES, contractor, and subcontractor employees who access data in this system must comply with the requirements of the Privacy Act of 1974, as well as the confidentiality standards under Section 183 of the ESRA (20 U.S.C. 9573).

All physical access to the NCES, contractor, and subcontractor sites where this system is maintained, is controlled and monitored by security personnel who check each individual entering the buildings for his or her employee or visitor badge.

7.5. Is the information in the system appropriately secured in accordance with the IT security requirements and procedures as required by Federal law and policy?

Yes

7.6. Has a risk assessment been conducted where appropriate security controls to protect against that risk have been identified and implemented?

Yes

7.7. Please describe any monitoring, testing or evaluation conducted on a regular basis to ensure the security controls continue to work properly at safeguarding the PII.

Monitoring, testing, and evaluation are ongoing as RTI follows the Department's Lifecycle Management framework and takes part in the ATO process which includes a rigorous assessment of the security and privacy controls and potential plans of actions and milestones to remediate any identified deficiencies. Additionally, NCES Applications at RTI is scanned regularly using automated tools to detect vulnerabilities. The results of the vulnerability scans are reviewed and addressed at the application and infrastructure levels.

RTI's Global Technology Solutions (GTS) Governance, Risk, and Compliance (GRC) department performs continuous monitoring on GTS security controls using annual security assessments that are conducted as self-assessments and independent assessments. Intrusion detection and monitoring systems are employed to review accesses and modifications and detect anomalies. Changes are captured and reviewed in audit logs for all software components. GTS utilizes firewalls with Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) functionality at key network boundaries within the network to monitor malicious or unwanted traffic. The IDS and IPS signature database is updated weekly to ensure the latest signatures are available and applied when required.

8. Auditing and Accountability

8.1. How does the system owner assess and ensure that the PII is used in accordance with stated practices in this PIA?

The system owner ensures that the information is maintained and used in accordance with stated practices in this PIA. An annual security assessment is conducted. In addition, every three years all the security controls are assessed for the system to maintain its Authorization to Operate. The Department's, contractor's, and subcontractors' employees who access data in this system must comply with the requirements of the Privacy Act and the confidentiality standards in section 183 of the ESRA (20 U.S.C. 9573), which provides criminal penalties for violations. Access to individually identifying data is strictly controlled. Staff with access to the system are required to complete annual security and privacy awareness training. In addition, they are required to have background clearance at the 5c level or higher.

8.2. Does the system owner continuously monitor and audit the privacy controls to ensure effective implementation?

Yes

8.3. What are the privacy risks associated with this system and how are those risks mitigated?

The main risk associated with this system is the potential for unauthorized individuals gaining access to PII of respondents. This PIA details the privacy controls and safeguards implemented for this system in order to mitigate privacy risk. These controls and safeguards work to protect the data and mitigate privacy risks. Mitigation of those risks at a system level includes selecting, implementing, assessing, and monitoring a full range of security and privacy controls, pursuant to National Institute of Standards and Technology (NIST) guidelines.

Access to PII is limited to staff who work on the study and need the PII to complete study tasks. All such staff must sign an affidavit of nondisclosure. Pursuant to the Education Sciences Reform Act of 2002 (20 U.S.C. 9573) these staff, as well as anyone who accesses NCES data, are subject to penalties if they willfully disclose respondent information or use the data for other than statistical purposes.

At the project level, the use of direct identifiers is minimized to the fullest extent possible. Direct identifiers, when needed, are used during actual data collection for sampling, consent, and contacting purposes. Within the NCES Applications at RTI system, any directly identifying information is stored separately from data collected in the surveys. Thus, direct identifiers are never associated with collected data in compiled data files. Study respondents are never identified in data files released for research purposes. This is true for both NCES restricted-use files, which are available only to researchers through license with NCES, and public-use files, which NCES makes freely available without restrictions.

All data included in data files intended for research use, both restricted use and public use, undergo a disclosure risk analysis and are subject to data perturbation techniques that must be reviewed and approved by the Institute of Education Sciences' Disclosure Review Board (IES DRB). All data are subject to review to minimize the risk that a respondent in a data file could be identified. Further, sensitive information is removed from public-use files. No data can be approved for release without the issuance of a "Safe-to-release" memo by the IES DRB chair. This memo confirms that the data files have undergone all steps necessary to minimize the risk that a respondent in a data file could be identified.