# NCER-NPSAS Grant Study

# Connecting Students with Financial Aid (CSFA) 2017: Testing the Effectiveness of FAFSA Interventions on College Outcomes

## Appendix D
## Confidentiality for Administrative Record Matching

## OMB # 1850-0931 v.2

Submitted by
National Center for Education Statistics
U.S. Department of Education

**October 2016**

## D.1 Develop Linkages with Administrative Data Sources

Linkages were developed with existing data sources to supplement the 2015-16 National Postsecondary Student Aid Study (NPSAS:16) student data collection. The Connecting Students with Financial Aid (CSFA) 2017 study will continue to collect supplemental data available through the Central Processing System (CPS), the National Student Loan Data System (NSLDS), and the National Student Clearinghouse (NSC) using procedures and processes developed and updated for the NPSAS:16 data collection.

NCES recognizes the great value added with the addition of data from specific administrative data sources as certain data, such as specific financial aid amounts and associated dates, can only be accurately obtained from sources other than the student or parent. Our postsecondary studies, including previous NPSAS studies, Beginning Postsecondary Student (BPS), and Baccalaureate and Beyond (B&B), have included file merges with many existing sources of valuable data, including Department of Education's (ED) Central Processing System (CPS) for Free Application for Federal Student Aid (FAFSA) data, the National Student Loan Data System (NSLDS), and ACT, the College Board, and the National Student Clearinghouse (NSC). For the Connecting Students with Financial Aid (CSFA) 2017 study, we plan to perform file merges with the following datasets: CPS, NSLDS, and NSC.

The Family Educational Rights and Privacy Act (FERPA) (34 CFR Part 99) allows the disclosure of information without prior consent for the purposes of NPSAS:16 according to the following excerpts: 34 CFR § 99.31 asks, "Under what conditions is prior consent not required to disclose information?" and explains in 34 CFR § 99.31(a) that "An educational agency or institution may disclose personally identifiable information from an education record of a student without the consent required by §99.30 if the disclosure meets one or more" of several conditions. These conditions include, at 34 CFR § 99.31(a)(3):

The disclosure is, subject to the requirements of §99.35, to authorized representatives of--

(i) The Comptroller General of the United States;
(ii) The Attorney General of the United States;
(iii) The Secretary; or
(iv) State and local educational authorities.

NPSAS:16 is collecting data under the Secretary's authority. Any personally identifiable information is collected with adherence to the security protocol detailed in 34 CFR § 99.35:

(a)(1) Authorized representatives of the officials or agencies headed by officials listed in §99.31(a)(3) may have access to education records in connection with an audit or evaluation of Federal or State supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs.

(2) The State or local educational authority or agency headed by an official listed in §99.31(a)(3) is responsible for using reasonable methods to ensure to the greatest extent practicable that any entity or individual designated as its authorized representative—
  (i) Uses personally identifiable information only to carry out an audit or evaluation of Federal- or State-supported education programs, or for the enforcement of or compliance with Federal legal requirements related to these programs;
  (ii) Protects the personally identifiable information from further disclosures or other uses, except as authorized in paragraph (b)(1) of this section; and
  (iii) Destroys the personally identifiable information in accordance with the requirements of paragraphs (b) and (c) of this section.

(b) Information that is collected under paragraph (a) of this section must—
(1) Be protected in a manner that does not permit personal identification of individuals by anyone other than the State or local educational authority or agency headed by an official listed in §99.31(a)(3) and their authorized representatives, except that the State or local educational authority or agency headed by an official listed in §99.31(a)(3) may make further disclosures of personally identifiable information from education records on behalf of the educational agency or institution in accordance with the requirements of §99.33(b); and
(2) Be destroyed when no longer needed for the purposes listed in paragraph (a) of this section.

**Secure Data Transfers.** NCES has set up a secure data transfer system, using the NCES member site with Secure Sockets Layer (SSL) technology, described above. The contractor will use this electronic system for submitting data containing potentially identifying information (such as SSNs, names, and dates of birth of our sample members) along with their survey ID (not the same ID that is available on the restricted-use data). Before being transmitted, files will be encrypted using FIPS 140-2 validated encryption tools. Data will be received from the NCES system as well. The system requires that both parties to the transfer be registered users of the NCES Members Site and that their Members Site privileges be set to allow use of the secure data transfer service as described above. This process will be used for all file matching procedures described below, except in instances when the vendor already has a secure data transfer system in place.

### D.2 File Merge with ED Central Processing System (CPS)

File merges will be performed with the CPS data containing federal student aid application information by the data collection contractor. The merge with CPS can occur at any time for any number of cases, provided that the case has an apparently valid SSN associated with it. A file will be sent to CPS and in return a large data file containing all students who applied for federal aid will be received. The data collection contractor has programs and procedures in place to prepare and

submit files according to rigorous CPS standards, and to receive and process data obtained from CPS.

A file will be electronically uploaded on the FAFSA secure web-site for matching which contains SSN and the first 2 letters of the sample member's last name (but no other information). Access to the site for the upload is restricted to authorized users who are registered and provide identification/authentication information (SSN, DOB, and personal identification number [PIN]) to the FAFSA data site. The file is retrieved by the Central Processing System or CPS (the FAFSA contractor data system) for linkage. The linked file, containing student aid applications for matched records, is then made available to us only through a secure connection (EdConnect) which requires username and password. All CPS files will be processed, edited, and documented for inclusion on the analytic data files. All CPS files will be processed, edited, and documented for inclusion in the final restricted use file (RUF).

### D.3 File Merge with National Student Loan Data System Disbursement (NSLDS)

A file merge will be conducted by the data collection contractor with the NSLDS to collect federal loan and Pell grant data. The resulting file will contain cumulative amounts for each student's entire postsecondary education enrollment. NCES has set up a secure data transfer system that uses their NCES member site and Secure Sockets Layer (SSL) technology. The system requires that both parties to the transfer be registered users of the NCES Members Site and that their Members Site privileges be set to allow use of the secure data transfer service. These privileges are set up and carefully controlled by the ED's Institute of Education Sciences (IES) NCES Chief Technology Officer (CTO), a service designed by ED/NCES specifically for the secure transfer of electronic files containing personally identifying information (i.e., data protected under the Privacy Act or otherwise posing risk of disclosure), and can be used for NCES-to-Contractor; Contractor-to-Subcontractor; Subcontractor-to-Contractor; and Contractor-to-Other-Agency data transfers. The party uploading the information onto the secure server at NCES is responsible for deleting the file(s) after the successful transfer has been confirmed. Data transfers using this system will include notification to the ED/IES, the NCES CTO, and the NCES Deputy Commissioner as well as the ED/NCES project officer. The notification will include the names and affiliations of the parties in the data exchange/transfer and the nature and approximate size of the data to be transferred. Programs have been developed to create the files for the merge and also to read the data receive. All matching processes are initiated by the data collection staff providing a file with one record per sample member to be merged.

### D.4 File Merge with the National Student Clearinghouse (NSC)

The National Student Clearinghouse will be used to obtain the *Student Tracker* data for persistence outcomes for the sampled cases.

The data collection contractor will first set up an account with the Clearinghouse which will enable sending and receiving of files securely over

encrypted FTPS connections. The file containing sensitive student identifiers (name, date of birth, and Social Security number) will be encrypted using FIPS 140-2 validated encryption tools then submitted to the Clearinghouse using their secure FTP site. All files received by the Clearinghouse will be securely stored using FIPS 140-2 validated AES encryption, the US federal encryption standard. Matched files, containing data on enrollment dates, institution names, and degrees completed, will be returned to the data collection contractor using the same secure FTP site.

### D.5 Processing Administrative Data

We will use verified Social Security numbers collected during NPSAS:16 to facilitate the batch mode processing that is suitable to many of these resources. We may need to match to a source (for example, CPS or NSLDS) more than once.

The data from all of these sources, as allowed by the vendor, will be delivered for inclusion on the RUF.