Privacy Impact Assessment (PIA) for the
Text Ed: Study of Text Messaging to Improve College Enrollment Rates Among Disadvantaged Adults
July 25, 2017

Contact Point
Melanie Ali
202-245-8345

System Owner
Brian Taylor

Author
Melanie Ali

Institute of Education Sciences
Reviewing Official
Kathleen Styles
Chief Privacy Officer
U.S. Department of Education
Please submit completed Privacy Impact Assessments to the Privacy Safeguards Division at privacysafeguards@ed.gov.

Please complete this Privacy Impact Assessment (PIA) on how information in identifiable form 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.

Introduction

1.1. Describe the system including the system name, system acronym, and a brief description of the major functions.

The system, “Text Ed: A Study of Text Messaging to Improve College Enrollment Rates Among Disadvantaged Adults,” will be used to rigorously evaluate whether the use of a promising, low cost text messaging strategy can help Education Opportunity Center (EOC) grantees meet the program’s goal of increasing college enrollment among disadvantaged adults. EOCs, which are part of the TRIO family of programs, provide informational services related to the college-going process and financial aid options. Most of the clients served by EOCs are adults who are low-income and potential first-generation college goers. This study is being conducted under legislative mandate to study promising practices with the potential to improve outcomes for TRIO programs.

The system will be used to examine the implementation of the text messages within the approximately 20 EOCs that volunteer to participate in the study, and the impact of the messages on clients’ rates of completion of the Free Application for Federal Student Aid (FAFSA) and enrollment in college. The system will include personally identifying information on adults who volunteer to participate in the study, including name, contact information, date of birth, sex, race/ethnicity, income, Social Security Number, educational background and plans, whether the participant is a caretaker for children, parents’ educational background, primary language spoke, FAFSA completion status, and college enrollment status. For study participants randomly assigned to receive the text messages, the system will also include information on the text messages, including the direction of the message (sent to client / received by client), the verbatim message content, and the date and time the message was sent.

1.2. Describe the purpose for which the personally identifiable information (PII)¹ is collected, used, maintained, or shared.

¹ 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
The data will be used to describe the implementation of the study’s text messaging intervention and to estimate the impact of the intervention on study participants’ rates of FAFSA completion and college enrollment. Along with enrolling in college, helping clients to access financial aid, a key goal of EOCs. The study complies with the legislative mandate that ED conduct studies of strategies to improve outcomes for TRIO programs.

PII will be collected in order to randomly assign the clients who volunteer to participate in the study to a group that gets the evaluation’s text messages or a group that does not, to obtain outcome data on FAFSA completion and college enrollment from the Office of Federal Student Aid and the National Student Clearinghouse, to describe the background characteristics of student participants, and potentially to create subgroups for analysis based on background characteristics. For clients who are assigned to receive the evaluation’s text messages, information on the text messaging will also be collected and maintained in order for the evaluation to describe implementation and appropriately interpret impact estimates.

Ultimately, the findings from this evaluation will be used to determine whether systematic, personalized text messaging is a useful enhancement to EOCs’ existing services. Aggregate findings from the study will be presented in a written report that will be publicly available and shared with the EOCs and relevant Department of Education offices. The data from the evaluation with PII will not be publicly released.

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

This is a new system.

1.4. Is this PIA new, or is it updating a previous version? If this is an update, please include the publication date of the original

This is new PIA.

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

The application is maintained by a contractor (MDRC) and is hosted in the Institute of Education Science’s (IES’) Data Center (IESDC).

2. Legal Authorities and Other Requirements

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

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. https://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf
2.1. What specific legal authorities and/or agreements permit and regulate the collection and use of data by the system?

The study is authorized under sections 171(b) and 173 of the Education Sciences Reform Act of 2002 (ESRA)(20 U.S.C. 9561(b) and 9563) and under Section 402(H) of the Higher Education Opportunity Act of 2008 (20 U.S.C. 1070a–18). These pieces of legislation provide IES with authority to conduct studies of promising strategies with potential to improve outcomes for TRIO programs.

**SORN**

2.2. Is the information in this system retrieved by name or personal identifier? If so this system will need to be covered by a Privacy Act System of Records Notice(s) (SORN(s))²? If no, explain why not. If yes, provide the SORN name and number, or indicate that a SORN is in progress.

A System of Records Notice (“Text Ed: A Study of Text Messaging to Improve College Enrollment Rates among Disadvantaged Adults” (18-13-41) is currently under Department review in preparation for publication in the Federal Register.

**Records Management**

*If you do not know your records schedule, please consult with your records liaison or RMHelp@ed.gov.*

2.3. Does a records retention schedule, approved by National Archives and Records Administration (NARA), exist for the records contained in this system? If yes, please provide the NARA schedule number.

Records are maintained and disposed of in accordance with the Department’s Records Disposition Schedule GRS 5.2, Item 011 Intermediary Records.

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

Records are maintained and disposed of in accordance with the Department’s Records Disposition Schedule GRS 5.2, Item 011 Intermediary Records.

---

² 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
3. Characterization and Use of Information Collection

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

The system will include personally identifying information on adults who volunteer to participate in the study, including name, contact information, date of birth, sex, race/ethnicity, income, Social Security Number, educational background and plans, whether the participant is a caretaker for children, parents’ educational background, primary language spoke, FAFSA completion status, and college enrollment status. For the subset of adults who volunteer to participate in the evaluation and are randomly assigned to receive the study’s text messages, the system will also include information related to the text messages. This includes the following: the direction of the message (sent to client / received by client), the verbatim message content; and the date and time the message was sent.

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

Yes.

3.3. What are the sources of information collected (e.g., individual, school, another agency, commercial sources, etc.), how is the information collected from stated sources (paper form, webpage, database, etc.), and how is this information validated or confirmed?3

The study includes individual-level data on adults who volunteer to participate in the study. These data will largely be obtained from administrative records, including the records of study EOCs, the Department’s Federal Student Aid Office, the National Student Clearinghouse, and the study’s text messaging platform provider. A small amount of background information on participants not available through EOC records will be collected via a participant survey. Data from the Federal Student Aid Office, the National Student Clearinghouse and the text messaging platform provider will be collected electronically. Data from EOC records and data from the participant survey will be collected electronically, to the extent possible. All data will undergo consistency and quality control checks.

Use

3.4. Describe how and why the system uses the information to achieve the purpose stated in Question 1.2 above

3 Examples include form filling, account verification, etc.
The information collected will be used to describe the implementation of the study’s text messaging intervention and to estimate the impact of the intervention on study participants’ rates of FAFSA completion and college enrollment. The study addresses the following research questions: Does providing personalized messages to EOC participants increase FAFSA completion rates? Does it increase college enrollment rates? What are participants’ experiences with the text messages (for instance, how often do they receive the messages? How often do they text back in response)? To what extent does the effectiveness of the messaging vary across EOC grantee sites? To what extent does the effectiveness vary across participant subgroups?

**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 the law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.*

3.5. Does the system collect Social Security Numbers? If so, explain the purpose of its collection, type of use, and any disclosures. *Please note if the system collects SSN, the PIA will require a signature by the Assistant Secretary or equivalent.*

Yes, the system collects Social Security Numbers. Many, but not all, EOCs already collect Social Security Numbers from clients, and only EOCs who are willing to do so will be included in the study. This is necessary in order that the evaluation will be able to accurately match study participants to records maintained by the Office of Federal Student Aid and the National Student Clearinghouse. Study participants will provide active consent to the disclosure of Social Security Numbers to the National Student Clearinghouse.

3.6. Specify any alternatives considered in the collection of SSN and why the alternatives were not selected.

Without the collection of Social Security Numbers, the evaluation will not be able to adequately examine impacts on FAFSA completion and college enrollment rates, which are key outcomes for the EOC program. Matching study participants to Federal Student Aid and National Student Clearinghouse records based on name and date of birth alone would substantially reduce the study’s ability to detect impacts and meet the legislative mandate to evaluate strategies to improve TRIO program outcomes.
4. Notice

4.1. How does the system provide individuals notice about the collection of PII prior to the collection of information (i.e. written Privacy Act notice, link to a privacy policy, etc.)? If notice is not provided, explain why not.

A system of records notice is being developed and will be published in the Federal Register. In addition, study participants will provide active consent prior to the collection of PII. The participant survey will contain the following language: According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The time required to complete this information collection is estimated to take an average of 5 minutes, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collected. Information collected for this study comes under the confidentiality and data protection requirements of the Institute of Education Sciences (The Education Sciences Reform Act of 2002, Title I, Part E, Section 183). Responses to this data collection will be used only for statistical purposes. The reports prepared for the study will summarize findings across the sample and will not associate responses with a specific Education Opportunity Center (EOC) grantee or individual. We will not provide information that identifies you or your EOC to anyone outside the study team, except as required by law.

4.2. Provide the text of the notice, or the link to the webpage where notice is posted.

When it is published, the system of records notice can be found at: www.ed.gov/notices

4.3. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

Participation in the study is voluntary. Clients may choose not to participate in the evaluation and thus not to provide PII to the project. Clients opt out of the project by not signing the informed consent. Clients who opt out can continue to receive EOCs’ typical services.

5. Information Sharing

Internal

5.1. Will information be shared internally with other ED organizations, if so, which ones?

Yes.

5.2. What information will be shared and with whom?
The names, dates of birth, and Social Security Numbers of study participants will be shared internally with the Federal Student Aid Office.

5.3. What is the purpose for sharing the specified information with the specified internal organizations? Does this purpose align with the stated purpose in Question 1.2 above?

This is for the purpose of matching participants to the administrative records of the Federal Student Aid Office, in order to obtain FAFSA completion outcomes for study participants. This aligns with the stated purpose in Question 1.2—specifically, estimating the impact of the text messaging on FAFSA completion rates among EOC participants, in order to inform improvements to the EOC program.

**External**

5.4. Will the information contained in the system be shared with external entities (e.g. another agency, school district, etc.)?

Yes.

5.5. What information will be shared and with whom?

The names, dates of birth, and Social Security Numbers of study participants will be shared with the National Student Clearinghouse.

As required by the Education Sciences Reform Act of 2002 (ESRA) (20 U.S.C. 9561(b) and 9563), a restricted use data file with study created identifiers will be available to researchers who are approved license holders and are in compliance with NCES data security procedures. The data file will exclude direct identifiers, including participant name, date of birth, and Social Security Number.

5.6. What is the purpose for sharing the specified information with the specified external entity? Does this purpose align with the stated purpose in Question 1.2 above?

The names, dates of birth and Social Security numbers of study participants will be shared with the National Student Clearinghouse in order to match participants to the National Student Clearinghouse’s administrative records on college enrollment. This will allow the study to estimate the impacts of the text messaging on college enrollment rates, consistent with the stated purpose in Question 1.2.
The restricted use data file will be for the purpose of allowing licensed researchers to replicate the study’s findings and for further research purposes.

5.7. How is the information accessed and used by the external entity?

Study participants’ names, dates of birth, and Social Security Numbers will be transmitted electronically from IES’ Data Center to the National Student Clearinghouse, using a secure file transfer protocol.

The restricted use data file will be provided to licensed researchers on encrypted, password-protected CD.

5.8. If the project is using the information for testing a system or for training/research purposes, what controls are in place to minimize the risk and protect the data?

The project is using the information for research purposes. The data will be collected and stored on IES’ Data Center. All physical access to the IES Data Center (IESDC), where this system of records is maintained, is controlled and monitored by security personnel. The IES Data Center has an Authority to Operate (ATO) at the FISMA Moderate Level. IES limits access to the IES Data Center to contract staff on a need-to-know basis, and controls individual users’ ability to access and alter records within the system. By hosting this application in the IES Data Center, the contractor is in compliance with the IT security requirements of the Department. Access to individually identifying data will be strictly controlled. The contractor’s employees who “maintain” (collect, maintain, use, or disseminate) data in this system shall comply with the requirements of the confidentiality standards in section 183 of the ESRA (20 U.S.C. 9573). Those who have access to the data will have obtained ED personnel security clearance at a level appropriate for access to personally identifiable information.

As required by the Education Sciences Reform Act of 2002 (ESRA) (20 U.S.C. 9561(b) and 9563), a restricted use data file with study created identifiers will be available only to researchers who are approved license holders and are in compliance with NCES data security procedures.

5.9. Does the system use “live” PII for the development or testing of another system? If so, please explain.

No.
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?

MDRC will enter into a Memorandum of Understanding with the National Student Clearinghouse, in order for the evaluation to share PII with the Clearinghouse and receive college enrollment data on study participants from the Clearinghouse.

As required by the Education Sciences Reform Act of 2002 (ESRA) (20 U.S.C. 9561(b) and 9563), a restricted use data file with study created identifiers will be available to researchers who are approved license holders and are in compliance with NCES data security procedures.

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

The contractor’s employees, the National Student Clearinghouse, and restricted use data file licensees must comply with the requirements of the confidentiality standards in section 183 of the ESRA (20 U.S.C. 9573).

6. Redress

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

A system of records notice will be published and procedures according to the SORN will be followed. The notice is currently undergoing internal ED review.

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

N/A, per footnote 4.

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

N/A, per footnote 4.

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?

---

4 If the system has a System of Records Notice (SORN), please provide a link to the SORN in Question 6.1 and proceed onto Section 7. Safeguards.
Yes, the system owner works closely with the Office of the Chief Information Officer to ensure that the required security controls are implemented enterprise-wide as well as specific to this system.

7.2. What procedures are in place to determine which users may access the information and how does the project determine who has access?

Access to individually identifying data is strictly controlled. IES limits access to the IES Data Center to ED and contract staff on a need-to-know basis, and controls individual users’ ability to access and alter records within the system and other procedures to ensure confidentiality of data. Users request access from the system owner and are only granted access after it is determined that they require access in order to perform valid work activity.

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

The IES Data Center complies with relevant security laws, OMB directives, FISMA, FEDRAMP and NIST standards. Implemented controls are comprised of a combination of management, operational, and technical controls, and include the following control families: access control, awareness and training, audit and accountability, security assessment and authorization, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protecting, physical and environmental protection, planning, personnel security, privacy, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management. All physical access to the IES Data Center, where this system of records is maintained, is controlled and monitored by security personnel. The contractor’s employees who “maintain” (collect, maintain, use, or disseminate) data in this system comply with the requirements of the confidentiality standards in section 183 of the ESRA (20 U.S.C. 9573).

7.4. Is an Authority to Operate (ATO) required? Has one been granted?

Yes, an ATO is required and has been granted to the IES Data Center.

7.5. Is the system able to provide an accounting of disclosures?

The system has audit and logging capabilities that would enable the system owner to provide an accounting of disclosures if requested under the Privacy Act.
8. **Auditing and Accountability**

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

The system owner operates the system proactively, reviewing the system’s privacy and security controls on an annual basis.

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

There are several privacy risks, both internally and externally that have been identified and mitigated. Risks include a breach of security safeguards, which could compromise the confidentiality integrity, and availability of information. The information in this system is protected from unauthorized disclosure through the implementation of applicable Privacy controls as identified within NIST SP 800-53 Rev 4.