



Privacy Impact Assessment

For

Even Start Classroom Literacy Interventions and Outcomes
(CLIO) Study

Date

December 6, 2006

System Owner:

Dr. Ricky Takai

Office of Institute of Education Sciences
U.S. Department of Education

1. What information will be collected for the system?

The system consists of: (1) The names and addresses of adults and children in the Even Start program who participate in the CLIO study; (2) demographic information such as race/ethnicity, age, and educational background for adults and children participating in the Even Start CLIO Study, for Even Start staff in programs participating in the CLIO study, and for the kindergarten and first grade teachers of CLIO children; (3) responses of adults participating in the Even Start CLIO study and project staff and teachers to interview questions; and (4) and the results of literacy assessments on adults and children participating in the Even Start CLIO study.

2. Why is this information being collected?

The information in this system is used for the following purposes: (1) To fulfill the requirements of the Even Start legislation for an evaluation of Even Start programs; and (2) To provide information on the effectiveness of specific family literacy interventions in those programs for use in improving the Even Start program.

3. How will the information be used?

The system contains records on adults and children in the William F. Goodling Even Start Family Literacy Programs (Even Start) program who participate in the CLIO study, on project staff from Even Start grantees participating in the CLIO study, and on the kindergarten and first grade teachers of CLIO children.

4. Will this information be shared with any other agency or entity? If so, with which agency or agencies/entities?

Information is disclosed internally to administer the program. However, it is not shared externally, except as required by law, or under the routine uses listed in the Privacy Act System of Records notice. These disclosures may be made on a case-by-case basis, or if the Department has complied with the computer matching requirements of the Act, under a computer matching agreement. Such disclosures may include: for litigation purposes, to the Department of Justice for FOIA advice, to contractors conducting Department business, for law enforcement, to a member of Congress at the request of the data subject, or to a consumer reporting agency regarding a valid and overdue claim.

5. Describe the notice or opportunities for consent that would be or are provided to individuals about what information is collected and how that information is shared with other organizations.

There is not notice or opportunities for consent since information is provided voluntarily.

6. How will the information be secured?

All physical access to the Department's site, and the site of the Department's contractor where this system of records is maintained, is controlled and monitored by security personnel. The computer system employed by the Department offers a high degree of resistance to tampering and circumvention. This computer system limits data access to Department and contract staff on a "need to know" basis, and controls individual users' ability to access and alter records within the system. The contractor, Westat, has established a set of procedures to

ensure confidentiality of data. The system ensures that information identifying individuals is in files physically separated from other research data. Westat will maintain security of the complete set of all master data files and documentation. Access to individually identifiable data will be strictly controlled. All data will be kept in locked file cabinets during nonworking hours, and work on hardcopy data will take place in a single room, except for data entry. Physical security of electronic data will also be maintained. Security features that protect project data include: password-protected accounts that authorize users to use the Westat system but to access only specific network directories and network software; user rights and directory and file attributes that limit those who can use particular directories and files and determine how they can use them; e-mail passwords that authorize the user to access mail services; and additional security features that the network administrator establishes for projects as needed. The contractor employees who maintain (collect, maintain, use, or disseminate) data in this system must comply with the requirements of the confidentiality standards in section 183 of the ESRA (20 U.S.C. 9573).

7. Is a system of records being created or updated with the collection of this information?

The system is covered under the system of records notice entitled Even Start Classroom Literacy Interventions and Outcomes (CLIO) Study, dated December 6, 2006, (71 FR 70745-70747).