Privacy Impact Assessment for the

Electronic Cohort Default Rate Appeals System (eCDR Appeals)

Date
December 7, 2007

Contact Point
System Owner: Sybil Phillips
Author: Catherine Connor (System Security Officer)

Federal Student Aid
U.S. Department of Education

1. What information will be collected for the system?

Categories of individuals covered by the system – The eCDR Appeals system contains records on borrowers who have received loans under the William D. Ford Direct Loan (Direct Loan) Program and the Federal Family Education Loan (FFEL) Program.

Categories of records in the system – The eCDR Appeals system contains records regarding: (1) Student/borrower identifier information including Social Security number and name; (2) loan information (e.g., last date of attendance, date entered repayment, default date) for each student/borrower loan counted in the cohort default rate of the school submitting the cohort default rate challenge or adjustment request; and (3) documentation submitted by a school or data manager to support its data allegation (e.g., enrollment verification, copies of cancelled checks, etc.).

2. Why is this information being collected?

The information contained in the records maintained in this system is used for the following purposes:

(1) To allow schools to electronically challenge their draft cohort default rate data via an incorrect data challenge, and electronically request an adjustment to their official cohort default rate data via an uncorrected data adjustment or new data adjustment;

(2) To allow Data managers to electronically view and respond to cohort default rate challenges and adjustment requests from schools. (Data managers are determined on the basis of the holder of the loan. For FFELP loans held by the lender or its guaranty agency, the guaranty agency is the Data manager for the purpose of the appeal. If the Department is the holder of the FFELP loan, then the Department is the Data manager. For Direct Loans, the Direct Loan servicer is the Data manager); and

(3) To allow Federal Student Aid to electronically view and respond to cohort default rate challenges and adjustment requests from schools.

3. How will FSA use this information?

The Department will disclose borrower loan records to the postsecondary school or Data manager responsible for the accuracy and completeness of the loan information, in order to obtain clarification or additional information to assist in determining the outcome of the school's allegations. This use is directly consistent with the programmatic purposes of the system to:

(1) Allow schools to electronically challenge their draft cohort default rate data via an incorrect data challenge, and electronically request an adjustment to their official cohort default rate data via an uncorrected data adjustment or new data adjustment;

(2) Allow managers to electronically view and respond to cohort default rate challenges and adjustment requests from schools; and

(3) Allow Federal Student Aid to electronically view and respond to cohort default rate challenges and adjustment requests from schools.

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

The Department of Education may disclose information contained in a record in this system of records under the routine users listed in the privacy Act System of Records notice without the consent of the individual if the disclosure is compatible with the purposes for which the record was collected. These disclosures may be made on a case-by-case basis or, if the Department has complied with the computer matching requirements of the Privacy Act, under a computer matching agreement.

Specific disclosures include the following:

- Program Disclosures
- Disclosure for Use by Other Law Enforcement Agencies
- Enforcement Disclosure
- Litigation and Alternative Dispute Resolution (ADR) Disclosure
- Freedom of Information Act (FOIA) Advice Disclosure
- Contract Disclosure
- Congressional Member Disclosure
- Disclosure in the Course of Responding to Breach of Data

Sharing of information will be done in compliance with the Privacy Act, and permitted routine use disclosure shall be compatible with the primary purpose(s) of collecting the information. Any contractor responsible for the operations of the eCDR Appeals system is held to the privacy and security requirements of the Department of Education in the handling of information collected through eCDR Appeals.

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

The eCDR Appeals system is a government agency database system with access limited to authorized users only. A warning banner reminds visitors of the consequences of unauthorized attempts to access the system:

This is a U.S. Federal Government owned computer system, for use by authorized users only. Unauthorized access violates 18 U.S. Code Section 1030 and other applicable statutes. Violations are punishable by civil and criminal penalties. Use of this system implies consent to have all activities on this system monitored and recorded, which can be provided as evidence to law enforcement officials.

Before being granted access to the system, authorized users must acknowledge and agree to comply with *eCDR Appeals System Rules of Behavior* (the Rules). Among other things, the Rules inform the users that the information contained in the eCDR Appeals system is protected by the Privacy Act of 1974, as amended; and stipulates that protecting this information, once it is entrusted to the eCDR Appeals user, becomes his or her responsibility.

The Rules outline good security practices expected of each authorized user, and specifically require all eCDR Appeals user to acknowledge the following criminal penalties imposed by the Privacy Act:

> *Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and may be fined not more than $5,000. (5 U.S.C 552a(i)(3)).*

Additionally, the Rules require Department employees and contractors authorized to access the eCDR Appeals system to acknowledge the following criminal penalties imposed by the Privacy Act:

> *Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000. (5 U.S.C 552a(i)(1)).*

The eCDR Appeals system will link to the Department's Privacy and Security Policy Notices (http://www.ed.gov/notices/privacy/index.html and http://www.ed.gov/notices/security/index.html) for easy reference by eCDR Appeals system users.

The eCDR Appeals system does not collect any information from visitors other than that required to authenticate them as an authorized user, and to monitor the site for any unauthorized access.

6. **How will the information be secured?**

All physical access to the Department's site, and the sites of the Department's contractors where this system of records is maintained, is controlled and monitored by security personnel who check each individual entering the building for his or her employee or visitor badge.

The computer system employed by the Department offers a high degree of resistance to tampering and circumvention. Records are stored in a database on the Department's secure servers, and via other controlled electronic media.

Access to records is limited to authorized personnel only. Authorized personnel retrieve records by school OPE-ID number and borrower Social Security number. They access records over the Internet using secure protocol with standard encryption protections. Individuals must review, and agree to follow the *eCDR Appeals System Rules of Behavior*. These outline good security practices and stipulate consequences of a failure to comply.

All users of this system of records are given a unique user identification. The Department's Federal Student Aid Information Security Privacy Policy requires and the system enforces a complex password policy. In addition, users are required to change their password at least every 60 to 90 days in accordance with the Department's information technology standards. At the principal site of the Department's contractor in Plano, Texas, additional physical security measures are in place and access is monitored 24 hours per day, 7 days a week.

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

Yes, a system of records is created with this collection of information. Users are provided notice of rights under the Privacy Act via links to the agency Privacy Act regulations (34 C.F.R. Part 5b.5) and to the Privacy Act system of records notice for the eCDR Appeals system.

8. List the web addresses (known or planned) that will have a Privacy Notice.

https://ecdrappeals.ed.gov