



Privacy Impact Assessment For

Educational Services of America/Edfinancial Services, LLC
(ESA/Edfinancial)

Date:
October 20 , 2011

Point of contact:
Tammy Morton
(202) 377-4653
Tammy.Morton@ed.gov

System Owner:
Keith Wilson
202-377-3591
Keith.Wilson@ed.gov

Author:
Wiley Hammer
Security and Risk Officer
Edfinancial Services, LLC
865-342-5233
whammer@edfinancial.com

**Office of
Federal Student Aid
U.S. Department of Education (ED)**

1. System Information. Describe the system - include system name, system acronym, and a description of the system, to include scope, purpose and major functions.

The ESA/Edfinancial system is used to service Federal Student Aid (FSA) Title IV student loans. This system processes all loan transfers, upload processing, maintenance transactions (i.e. demographic data, enrollment data, deferments, etc.), payment postings, due diligence and records borrower communications. ESA/Edfinancial communicates with the internal FSA platforms, borrowers, educational institutions, lending institutions, other loan servicers, third-party data providers, consumer reporting agencies, guarantors and government agencies (as permitted by the Federal Privacy Act of 1974). Channels of communication include mail, phone calls, a secure borrower website, email and secure data transfer links.

2. Legal Authority. Cite the legal authority to collect and use this data. What specific legal authorities, arrangements, and/or agreements regulate the collection of information?

The following provide legal authority for ESA/Edfinancial to collect and use the associated data:

- Titles II, IV-A, IV-B, IV-D, IV-E and V-C of the Higher Education Act (HEA) (20 U.S.C. 1024, 1070a, 1070b-1070b-4, 1070c-1070c-4, 1070c-3a, 1071-1087-4, 1087a-1087j, and 1087aa-1087ii, and 1104 (1998); 31 U.S.C. Chapter 37).
- Higher Education Act of 1965 as amended §428 and §484(b)(4) and Code of Federal Regulations: 34 CFR §668 and §682

3. Characterization of the Information. What elements of Personal Identifiable Information (PII) are collected and maintained by the system (e.g., name, social security number, date of birth, address, phone number, etc.)? What are the sources of information (e.g., student, teacher, employee, university)? How is the information collected (website, paper form, on-line form)? Is the information used to link or cross-reference multiple databases?

Personally identifiable information (PII) collected for borrowers, students, and references, depending on the loan type, may include: full name, maiden name, social security number (SSN), physical home and business address, home and business phone numbers, date of birth, driver's license number, bank account information, account number, disbursement amounts, account balances, outstanding loan payment amount, monthly loan payment amount, loan status, forbearance status, deferment status, separation date, grace period, and delinquency status, citizenship status and email address.

ESA/Edfinancial collects elements of PII from the following:

- from the prior servicer at the time the loan is converted to ESA/Edfinancial for servicing
- bulk file transfers from third-party data providers
- educational institutions and other loan servicers
- US Department of Treasury (Treasury)
- Borrowers, through electronic mail and paper correspondence

The borrower SSN and/or account number is used to cross-reference multiple systems described in question #1 above, other PII such as date of birth and name may also be used for secondary matches.

4. Why is the information collected? How is this information necessary to the mission of the program, or contributes to a necessary agency activity. Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The information is necessary to support the mission of the Agency in order to comply with the HEA policies, regulations and statutes. The PII is necessary to properly service loans according to the statute and regulatory requirements of the Title IV program.

The borrower name, address, email address, and phone numbers are essential for communicating with the borrower and performing collection activities. Endorser and references name, address, and phone numbers are used to reach the borrower when conventional methods fail.

The risk is that PII may be obtained by an unauthorized party to commit fraud and identify theft. The following are mitigation steps in place.

- The ESA/Edfinancial Corporate Security Policy is in place which includes procedural, technological and physical controls to ensure required and necessary security protocols are continuously maintained.
- Employees with the ability to access this information require a personnel security clearance before access is granted.
- System access is assigned based on job function requirements and are maintained through access controls.
- The change management process includes segregation of duties.
- Employees are also required to complete a Security and Awareness Training annually.
- Physical access to areas where PII data is available is secured with a security badge system to limit physical access to areas as required.
- Annual risk assessments are performed.
- Security vulnerabilities are identified, tracked and mitigated.

5. Social Security Numbers. If an SSN is collected and used, describe the purpose of the collection, the type of use, and any disclosures. Also specify any alternatives that you considered, and why the alternative was not selected.

The SSN is the unique identifier for Title IV programs and is required by program participants and their trading partners to satisfy borrower eligibility, loan servicing, and loan status reporting requirements under law and regulations. Trading partners include the Department of Education, Internal Revenue Service, and institutions of higher education, nationwide consumer reporting agencies, lenders, and servicers.

Borrowers (and endorsers, if applicable) are advised of the collection and use of the SSN in the promissory note materials of their Title IV program loans. In accordance with state laws regarding the use of SSN's a proprietary account number is assigned by ESA/Edfinancial and utilized for all borrower and endorser communications in lieu of the SSN except where a SSN is required on a federal form. The proprietary account number is also used for the purposes of internal reporting and communications. The HEA Act of 1965 and Privacy Act of 1974 provide the disclosure information.

6. Uses of the Information. What is the intended use of the information? How will the information be used? Describe all internal and/or external uses of the information. What types of methods are used to analyze the data? Explain how the information is used, if the system uses commercial information, publicly available information, or information from other Federal agency databases.

The SSN is used to uniquely identify the borrower, student, or endorser and the applicable account. In addition to the SSN, the other PII listed above in #3 is used to fully satisfy all loan servicing and reporting requirements of Title IV programs and other applicable laws and regulations. These uses

include the following: verification of identity; determination of benefits, such as deferment, forbearance, discharge, or forgiveness; loan status reporting; Internal Revenue Service Forms 1098 and 1099 for income reporting; location efforts for borrowers with invalid contact information (skip borrowers); and collection of a delinquent loan.

7. Internal Sharing and Disclosure. Which internal ED organizations will the information being shared? What information is shared? For what purpose is the information shared? Describe the risks to privacy for internal sharing and disclosure and describe how the risks were mitigated.

The internal ED organizations this information is shared with include the National Student Loan Data System (NSLDS) and the Debt Management Collection System (DMCS).

The information shared is sensitive PII (borrower data) and is shared for the purpose of satisfying all loan servicing and reporting requirements of Title IV programs and other applicable laws and regulations

8. External Sharing and Disclosure. With what external entity will the information be shared (e.g., another agency for a specified programmatic purpose)? What information is shared? For what purpose is the information shared? How is the information shared outside of the Department? Is the sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU) or other type of approved sharing agreement with another agency? Describe the risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

A signed MOU and Interconnection Security Agreement (ISA) with the Financial Management System (FMS) office of the Department of Treasury will be executed.

The system shares various PII elements with the following external entities: U.S. Department of Treasury (Treasury), Internal Revenue Service, (IRS), institutions of higher education, consumer credit reporting agencies, lenders, guaranty agencies and servicers.

PII is shared for the purpose of servicing borrower account management, loan conversion/de-conversion, interim/repayment servicing, payment posting, deferment and forbearance processing, letter generation, call scheduling, loan transfer/put/un-put activities, collection, skip-tracing, claims and correspondence history files.

Risks to sharing this information are mitigated through secure and encrypted transmissions, segregation of duties, and signed agreements that clearly delineate each party's security and privacy responsibilities. ESA/Edfinancial utilizes virus, phishing, malware, worm detection technology to protect data at rest within the system boundary

9. Notice. Is a notice provided to the individual prior to collection of their information (e.g., a posted Privacy Notice)? What opportunities do individuals have to decline to provide information (where providing the information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent?

Individuals are provided with a notice as required by the Privacy Act of 1974 as part of the promissory note materials. The notice explains what types of PII are being collected, why PII is being collected and how the PII will be used. Upon a loan being converted to ESA/Edfinancial for servicing as a government owned loan, borrowers will be provided with the Department of Education's privacy policy in accordance with the Gramm-Leach-Bliley Act (GLBA), and annually thereafter.

10. Web Addresses. List the web addresses (known or planned) that have a Privacy Notice.

The ESA/Edfinancial privacy policy will be available on Portal.edservicing.com

11. Security. What administrative, technical, and physical security safeguards are in place to protect the PII? Examples include: monitoring, auditing, authentication, firewalls, etc. Has a Certification and Accreditation (C&A) been completed? Is the system compliant with any federal security requirements? If so, which federal security requirements?

ESA/Edfinancial complies with the requirements of the Federal Information Security Management Act, which requires that comprehensive security and privacy controls be in place and that the proper implementation and operation of these controls be certified by an independent third party.

Physical access to areas where PII data is available is secured with a security badge system to limit physical access to areas as required.

ESA/Edfinancial employs the following technical safeguards:

- Firewalls and existing proxy servers are in place to control external access to internal resources
- Connections to the Internet, or other external networks or information systems, occur through controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels). The operational failure of the boundary protection mechanisms does not result in any unauthorized release of information outside of the ESA/Edfinancial boundary.
- ESA/Edfinancial prevents public access into the organization's internal networks except as appropriately mediated.
- All routers, switches and firewalls are configured to allow only specifically authorized services and traffic (Deny-By-Default).

Additional security and privacy controls are listed in the answer to question 4.

12. Privacy Act System of Records. Is a system of records being created or altered under the Privacy Act, 5 U.S.C. 552a? Is this a Department-wide or Federal Government-wide SORN? If a SORN already exists, what is the SORN Number?

ESA/Edfinancial will be covered under the System of Records Notice, Common Services for Borrowers (CSB) Contract, 18-11-16, 71 FR 3503-3507.

13. Records Retention and Disposition. Is there a records retention and disposition schedule approved by the National Archives and Records Administration (NARA) for the records created by the system development lifecycle AND for the data collected? If yes – provide records schedule number:

Records will be covered under the following schedule: ED 072 FSA Application, Origination and Disbursement Records, NARA Disposition Authority N1-441-09-23.

Certifying Officials' Signatures

Paula Elia
Senior Program Official

10-24-11
Date

Sammy Norton
Computer Security Officer/ Information System
Security Officer

10-24-11
Date

For systems that collect, maintain and or transfer SSNs:

Chy Long
Assistant Secretary or designee

10/31/2011
Date

Privacy Advocate

Date