Privacy Impact Assessment

For: Health Education Assistance Loans (HEAL)

Online Processing System (HOPS)

Date: May 11, 2016

Point of Contact: Valerie Hough Cromartie

System Owner: Diana O'Hara

Author: Valerie Hough Cromartie

Office of Federal Student Aid

U.S. Department of Education

1. **System Information.** Describe the system - include system name, system acronym, and a description of the system, to include scope, purpose and major functions. Indicate whether the system is new or existing, and whether or not the PIA is new or being updated from a previous version; specify whether the system is 'agency' or 'contractor.

   Health Education Assistance Loans (HEAL) Online Processing System (HOPS) is an automated system that tracks and maintains HEAL-related loan information. HEAL information consists of: Borrowers; Loans; Claims; Litigations against defaulted loans; Lenders; and Educational Institutions receiving loan funds. Loan servicing organizations use HOPS information to update and verify the accuracy or status of loan guarantees. HOPS is an existing system and this is an updated PIA from the one that was previously created by the U.S. Department of Health and Human Services (HHS).

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?

   AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

   Sections 701 and 702 of the Public Health Service Act, as amended (42 U.S.C. 292 and 292a), which authorize the establishment of a Federal program of student loan insurance; Section 715 of the Public Health Service Act, as amended (42 U.S.C. 292n), which directs the Secretary to require institutions to provide information for each student who has a loan; Section 709 of the Public Health Service Act, as amended (42 U.S.C. 292h), which authorizes disclosure and publication of HEAL defaulters; and the Debt Collection Improvement Act (31 U.S.C. 3701 and 3711–3720E).[1]

   E-Government Act of 2002

   For all PIAs Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C.Ch 36) requires that the Office of Management and Budget issue guidance to agencies on implementing the privacy provisions of the E-Government Act. The E-Government Act requires agencies to conduct PIAs for their electronic information systems and collections.

   The Privacy Act of 1974

   The Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual.

   The Privacy Act requires that agencies give the public notice of their systems of records by publication in the Federal Register. The Privacy Act prohibits the disclosure of a record about an individual from a system of records absent the written consent of the individual, unless the disclosure is pursuant to one of twelve statutory exceptions. The Act also provides individuals with a means by which to seek access to and amendment of their records, and sets forth various agency record-keeping requirements.

[1] Federal Register / Vol. 75, No. 20 / Monday, February 1, 2010 / Notices. http://www.gpo.gov/fdsys/pkg/FR-2010-02-01/pdf/2010-1970.pdf

3. **Characterization of the Information.** What elements of personally identifiable information (PII) are collected and maintained by the system (e.g., name, social security number, date of birth, address, phone number)? 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?

   Records in the system contain: name, social security number or other identifying number, birth date, demographic background, educational status, loan location and status, and financial information about the individual for whom the record is maintained; the information contains lender and school identification[2]. The full list of PII data is listed below:

   Required Data Items:
   - BORROWER ID
   - BORROWER SSN
   - BORROWER LASTNM
   - BORROWER FIRSTNM
   - BORROWER ADDR1
   - BORROWER CITY
   - BORROWER ZIP
   - BORROWER BIRTH_DT
   - BORROWER AGRAD_GRAD_DT

   HOPS obtains the borrowers' PII only from the HEAL Servicers and does not obtain PII directly from individuals.

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 any type of data collected, discuss the privacy risks (internally and/or externally) identified and how they were mitigated.

   The purpose of the system is 1) to identify students participating in the HEAL program 2) to determine eligibility of loan applicants and to compute insurance premium for federal insurance 3) to monitor the loan status of HEAL recipients, which includes the collection of overdue debts owed under the HEAL program 4) to compile and generate managerial and statistical reports 5) process claims and 6) produce an annual report that contains aggregate information but no individual borrower can be identified in this report. The categories of records in the system contains name , SSN, birth date, demographic background, educational status, loan location and status, and financial information about the individual for whom the record is maintained, lender and school identification. Disclosure of the applicant's SSN is mandatory for participation in the HEAL program as provided for by Section 4 of the Debt Collection Act of 1982. Submission of PII is mandatory Applicant Form HRSA-700 states the SSN will be used to verify the identity of the applicant and as an account number throughout the life of the loan to record necessary data accurately. Applicants are advised that failure to provide his/her SSN will result in the denial of the individual to participate in the HEAL program.

   The information is necessary to the mission of the Agency in order to comply with the HEA policies, regulations, and statues.

   Privacy risks would result from a breach of the HEAL Online Processing System's security safeguards, which could compromise the confidentiality, integrity, and availability of

[2] Federal Register / Vol. 75, No. 20 / Monday, February 1, 2010 / Notices.

information. The most likely method of breach would be through unauthorized access that would enable an adversary to disclose, damage the integrity of, or prevent the availability of information. Another type of risk would be a man-made or natural disaster destroying the data center or place of business.

Key Risk Mitigation Measures include:

- Physical security, such as guards, access badges, and security cameras protect against unauthorized access to component facilities
- Unauthorized access to the system itself is addressed by network intrusion detection systems, firewall/firewall log monitoring, malware detection and removal software, Virtual Private Networks (VPN), and encryption at the perimeter
- All external electronic transmissions used to receive or send PII data are encrypted
- To protect unauthorized access to the HOPS, audit logs are maintained and reviewed at regular intervals and HOPS access is restricted by limiting the access based on the principle of least privilege
- All FSA and contractor personnel are required to obtain government security clearance, to read and acknowledge the rules of behavior, and to complete an initial security training and awareness course as well as periodic refresher training
- The HOPS infrastructure is located in facilities that leverage appropriate environmental controls
- HOPS maintains appropriate systems for redundancy and failover
- HOPS maintains incident response, disaster recovery, and business recovery plans to minimize impact of any failures/outages from man-made or natural disasters
- FSA and Contracting Companies require annual security training for all employees and implement security controls as mandated by the Federal Information Security Management Act (FISMA). Implementation of these controls and associated risks and mitigation is reflected in required security documentation. Additional information regarding risk mitigation and security safeguards is provided in Section 11.

5. **Social Security Number (SSN).** 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. If system collects SSN, the PIA will require a signature by the Assistant Secretary. If no SSN is collected, no signature is required.

   The SSNs for recipients of Health Education Assistance Loans are maintained by the servicers assigned to the borrower. The SSN is the unique identifier for Title IV programs and its use 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 (IRS), institutions of higher education, national credit bureaus, lenders and servicers.

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 PII information is used for identification when the program receives claim submissions. Section 709(c)(2) of the Act is directed that HHS may release information on borrowers excluded

for Medicare and Medicaid to relevant federal agencies, schools, school associations, professional associations, state licensing board, hospitals that borrowers are associated with and other relevant organizations. We can release defaulter's name, SSN, last known address, name and location of school attended and amount of debt. If an individual seeks to find out if the system contains records about that individual, the system manager is contacted by a request in person that requires at least one tangible identification card; or request by mail containing the name and address of the requester, birth date, at least one tangible identification card, and signature. The HEAL Regulations do not state anything with regard to PII. Each of our Servicers handle PII differently.

7. Internal Sharing and Disclosure. With which internal ED organizations will the information be shared? What information is shared? For what purpose is the information shared?

Internal sharing: Loan Servicer personnel for verification of loan data. HEAL and Division of Financial Operations staff to process claims and claim payments.

The purpose information is shared:

1. To identify borrowers participating in the HEAL Program;

2. To monitor the loan status of HEAL recipients, which includes the collection of overdue debts owed under the HEAL Program; and

3. To compile and generate managerial and statistical reports.

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 or other type of approved sharing agreement with another agency?

The System is located externally at:

Division of Infrastructure Services (DIS), Hosting Branch (HB)
Health Resources and Services Administration Office of Technology
Room: 03E01 Staging/Dev. Rm#1, Inside Room: 03E03 Data Center
Parklawn Building, 5600 Fishers Lane
Rockville, MD 20857

• Records are also located at contractor sites. A list of contractor sites where individually identifiable data are currently located is available upon request to the System Manager.

• Washington National Records Center, 4205 Suitland Road, Suitland, MD 20409

THE PURPOSES OF EXTERNAL SHARING AND DISCLOSURE[3]:

1. Disclosure may be made to Federal, State, or local agencies, to private parties such as relatives, present and former employers, business and personal associates, educational and financial institutions, and collection agencies. The purpose of such disclosures is to verify the identity of the loan applicant, to determine program eligibility and benefits, to enforce the conditions or terms of the loan, to counsel the borrower in repayment efforts, to investigate possible fraud and abuse, to verify compliance with program regulations, and to locate delinquent borrowers through pre-claims assistance. Information may be disclosed to educational or financial institutions to assist them in loan management.

[3] Federal Register / Vol. 75, No. 20 / Monday, February 1, 2010 / Notices

2. Disclosure may be made to a Congressional office from the record of an individual in response to an inquiry from the Congressional office made at the request of that individual.

3. The Department of Health and Human Services (HHS) may disclose information from this system of records to the Department of Justice, or to a court or other tribunal, when: (a) HHS, or any component thereof; or (b) any HHS employee in his or her official capacity; or (c) any HHS employee in his or her individual capacity where the Department of Justice (or HHS, where it is authorized to do so) has agreed to represent the employee; or (d) the United States or any agency thereof where HHS determines that the litigation is likely to affect HHS or any of its components, is a party to litigation or has an interest in such litigation, and HHS determines that the use of such records by the Department of Justice, the court or other tribunal is relevant and necessary to the litigation and would help in the effective representation of the governmental party, provided, however, that in each case, HHS determines that such disclosure is compatible with the purpose for which the records were collected.

4. In the event that a system of records maintained by this agency to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule or order issued pursuant thereto, the relevant records in the system of records may be referred to the appropriate agency, whether Federal, State or local, charged with enforcing or implementing the statute or any rule, regulation or order issued pursuant thereto.

5. FSA will disclose from this system of records a delinquent debtor's name, address, Social Security number, and other information necessary to identify him/her; the amount, status, and history of the claim, and the agency or program under which the claim arose, as follows: (a) To another Federal agency so that agency can effect a salary offset for debts owed by Federal employees; if the claim arose under the Social Security Act, the employee must have agreed in writing to the salary offset:

(b) To another Federal agency so that agency can affect an authorized administrative offset; i.e., withhold money payable to, or held on behalf of, debtors other than Federal employees.

(c) To the Treasury Department, Internal Revenue Service (IRS), to request a debtor's current mailing address to locate him/her for purposes of either collecting or compromising a debt or to have a commercial credit report prepared.

6. Records may be disclosed to the Office of Management and Budget for auditing financial obligations to determine compliance with programmatic, statutory, and regulatory provisions.

7. FSA may disclose information from this system of records to a consumer reporting agency (credit bureau) to obtain a commercial credit report for the following purposes:

(a) To establish creditworthiness of a loan applicant; and

(b) To assess and verify the ability of a debtor to repay debts owed to the Federal Government. Disclosures are limited to the individual's name, address, Social Security number and other information necessary to identify him/her; the funding being sought or amount and status of the debt; and the program under which the application or claim is being processed.

8. FSA may disclose to the Internal Revenue Service (IRS), U.S. Department of the Treasury (Treasury Department), information about an individual applying for a loan under any loan program authorized by the Public Health Service Act to find out whether the loan applicant has a delinquent tax account. This disclosure is for the sole purpose of determining the applicant's creditworthiness and is limited to the individual's name, address, Social Security number, other

information necessary to identify him/her, and the program for which the information is being obtained.

9. FSA will report to the IRS, Treasury Department, as taxable income, the written-off amount of a debt owed by an individual to the Federal Government when a debt becomes partly or wholly uncollectible—either because the time period for collection under the statute of limitations has expired, or because the Government agrees with the individual to forgive or compromise the debt.

10. FSA will disclose to debt collection agents, other Federal agencies, and other third parties who are authorized to collect a Federal debt, information necessary to identify a delinquent debtor. Disclosure will be limited to the debtor's name, address, Social Security number, and other information necessary to identify him/ her; the amount, status, and history of the claim, and the agency or program under which the claim arose.

11. FSA will disclose information from this system of records to any third party that may have information about a delinquent debtor's current address, such as the U.S. Postal Service, a consumer reporting agency (credit bureau), a State motor vehicle administration, a professional organization, an alumni association, etc., for the purpose of obtaining the debtor's current address. This disclosure will be limited to information necessary to identify the individual (defaulter's name, latest known City and State of residence, total amount of the HEAL debt).

12. Records may be disclosed to Department contractors and subcontractors for the purpose of assisting HEAL program managers in collating, compiling, aggregating, or analyzing records used in administering the HEAL program. Contractors maintain, and are also required to ensure that subcontractors maintain, Privacy Act safeguards with respect to the records.

13. FSA may disclose from this system of records to the IRS, Treasury Department:

(a) A delinquent debtor's name, address, Social Security number, and other necessary information to identify the debtor;
(b) the amount of the debt; and
(c) the program under which the debt arose, so that the IRS can offset against the debt any income tax refunds which may be due to the debtor.

14. FSA may disclose the complete loan file of defaulted HEAL recipients to potential purchasers of HEAL loans to enable them to value and price the loans, and to actual purchasers to enable them to collect the defaulted loans. The purpose of this disclosure will be to facilitate the sale and collection of defaulted HEAL loans. Potential purchasers are required to maintain Privacy Act safeguards with respect to the records.

15. In accordance with the directive in 42 U.S.C. 292h(c)(1), the names of HEAL borrowers who are in default will be published in the Defaulted Borrowers Web site, http://www.defaulteddocs.dhhs.gov, by city and State along with the amounts of their HEAL debts. The individual's address also may be published if the address is a matter of public record as a result of legal proceedings having been filed concerning the individual's HEAL debt.

16. In accordance with the directive in 42 U.S.C. 292h(c)(2), disclosure may be made to relevant Federal agencies, schools, school associations, professional and specialty associations, State licensing boards, hospitals with which a HEAL defaulter may be associated, and other similar organizations.

17. To appropriate Federal agencies and Department contractors that have a need to know the information for the purpose of assisting the Department's efforts to respond to a suspected or confirmed breach of the security or confidentiality of information maintained in this system of records, and the information disclosed is relevant and necessary for that assistance.

DISCLOSURE TO CONSUMER REPORTING AGENCIES:

Disclosures pursuant to 5 U.S.C. 552a(b)(12), (as set forth in 31 U.S.C. Section 3711(e)): Disclosures may be made from this system to ‘‘consumer reporting agencies’’ as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a(f)) or the Debt Collection Improvement Act (31 U.S.C. 3701(a)(3)).

The purposes of these disclosures are:

1. To provide an incentive for debtors to repay delinquent Federal Government debts by making these debts part of their credit records; and

2. To enable FSA to improve the quality of loan and scholarship decisions by taking into account the financial reliability of applicants.

Disclosure of records will be limited to the individual's name, Social Security number (SSN), and other information necessary to establish the identity of the individual, the amount, status, and history of the claim, and the agency or program under which the claim arose.

9. Notice. Is 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?

HOPS is not available to the general public but is available to designated Loan Servicers. If someone felt their PII had been inappropriately obtained, used, or disclosed, they could contact us directly or their loan servicer who provided us with the information. The complaint process could come in the form of a letter or a congressional request and with a valid borrower-release, the complaint would be investigated.

10. Web Addresses. List the web addresses (known or planned) that have a Privacy Notice.
The HEAL Online Processing System's web address is, https://heal.hrsa.gov/hops/login.aspx.

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 C&A been completed? Is the system compliant with any federal security requirements?
In accordance with the Federal Information Security Management Act of 2002 (FISMA), every FSA system must receive a signed Authority to Operate (ATO) from a designated FSA official. The ATO process includes a rigorous assessment of security controls, a plan of actions and milestones to remediate any identified deficiencies, and a continuous monitoring program. HOPS is scheduled to receive its ATO on May 20, 2016.

FIMSA controls implemented comprise 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 protection, physical and environmental protection, planning, personnel security, risk assessment, system and services acquisition, system and communications protection, system and information integrity, and program management.

Additionally, the following specific controls are applied:

The system uses strong encryption for all communications (HTTPS) from the time the user logs on until they log off. Usernames and passwords are sent encrypted as well as all data transferred

during the session. This is accomplished using Secure Sockets Layer (SSL) technology. PII data fields in the HOPS system are encrypted while the data is at rest. PII is transmitted to HRSA using encrypted, secure protocols.

The system is housed in a government facility with physical controls. Access to the HEAL office space is controlled with a building pass card and cipher locks.

The concept of "least privilege" provides users a minimal set of system access rights based on their role. Access to additional resources or information is granted upon approval by the resource owner (supervisor). Unique UserIDs and passwords permit only authorized users to access the system. Select users are individually assigned write, create and update privileges to loan data based on their functional role. Accounts are reviewed annually to ensure that least privilege is granted, and roles and responsibilities have not changed.

OIT provides connectivity to the HRSA LAN access to the HEAL-HOPS System by authorized Internal Users, and by authorized Internet Access for External Users. There is no information available for use by the general public.

An "inactivity time out" capability disables unattended computers to prohibit unauthorized access to PII.

All authorized system users, contractors and federal, are required to sign a "Rules of Behavior" when requesting user access. The Statement of Work (SOW) provides guidance for contractors to comply with HEAL-HOPS security requirements. The contractor shall comply with existing federal and departmental laws, regulations, and requirements.

12. **Privacy Act System of Records.** Is the information within the system retrieved by personal identifier? 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?

    Yes the system of records was created under the **Act, 5 U.S.C. 552a.** Enacted in 1974, the Privacy Act, 5 U.S.C. 552a, provides US citizens or permanent resident aliens (PRAs) with a right of access to information concerning themselves that is maintained by any agency in the Executive Branch of the federal government. The Act also established controls over what personal information the federal government collects and how it uses or discloses that information.

    The Systems of Records Notices (SORN) identify the legal authority for collecting and storing the records, what kinds of information is collected, and how the records will be used.

    The HOPS SORN, Health Education Assistance Loan (HEAL) program (SORN# 18-11-20) was published in the Federal Register on June 26, 2014.

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:

HOPS was transferred from the U.S. Department of Health and Human Services on July 1, 2014. FSA is working with the Records Officer and National Archives and Records Administration (NARA) to obtain the appropriate retention value[4].

[4] Federal Register / Vol. 75, No. 20 / Monday, February 1, 2010 / Notices