Privacy Impact Assessment (PIA)

for the

Health Education Assistance Loan (HEAL) Online Processing System (HOPS)

December 18, 2023

Point of Contact

Contact Person: David Christie
Title: Information System Owner
Email: David.Christie@ed.gov

System Owner

Name: David Christie
Title: Information System Owner
Principal Office: Federal Student Aid

Submit completed Privacy Impact Assessments to the Privacy Office at privacysafeguards@ed.gov

*Please complete this **Privacy Impact Assessment (PIA)**, which describes how personally identifiable information (PII) 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, answer with N/A.

- **Please ensure all responses are written in plain language. Write out all acronyms on first use and use acronyms consistently thereafter.**

- **For questions that are identical to those in the Privacy Threshold Analysis (PTA), please review the responses provided in the most recently approved PTA, determine whether the responses remain accurate, and, if so, use the same response in the PIA.**

1. Introduction

1.1. Describe the project or program that uses this information technology (IT) system, including the purpose of the project or program.

The Federal Health Education Assistance Loan (HEAL) program, authorized under Sections 701-720 of the Public Health Service Act, insured the loans provided by private lenders to students attending schools of eligible health professions. From fiscal year 1978 through fiscal year 1998, the HEAL program insured loans made by participating lenders to eligible graduate students in schools of medicine, osteopathy, dentistry, veterinary medicine, optometry, podiatry, public health, pharmacy, chiropractic medicine, or in programs in health administration and clinical psychology. On July 1, 2014, the HEAL program was transferred from the U.S. Department of Health and Human Services (HHS) to the U.S. Department of Education (Department). Authorization to fund new HEAL loans to students expired September 30, 1998. Provisions of the HEAL legislation allowing for the refinancing or consolidation of existing HEAL loans expired September 30, 2004. However, the reporting, notification, and recordkeeping burden associated with refinancing HEAL loans, servicing outstanding loans, and administering and monitoring of the HEAL program regulations continues. In addition, the Department analyzes and reviews claim packages received from lenders on defaulted loans.

The HOPS system was maintained by the HHS until September 30, 2017, when the Department assumed this responsibility.

1.2. How does the IT system function to support the project or program as described in Question 1.1?

The HEAL Online Processing System (HOPS) is an automated system that tracks and maintains HEAL-related information regarding the servicing of outstanding loans until they are paid off. HOPS contains information regarding recipients, loans, claims, litigations against defaulted loans, lenders, and educational institutions where recipients

are studying or have studied. Information is collected from loan servicers, not directly from individual recipients. Loan servicing organizations use HOPS to update and verify the accuracy or status of loan guarantees.

Access to HOPS for both loan servicers and FSA staff requires authentication through the Federal Student Aid (FSA) Access and Identity Management System (AIMS). Agents of loan servicing organizations can only view the loan information of recipients that they service. For defaulted loans, HHS performs collection actions and updates the status of these actions within HOPS.

FSA staff use the system to track the performance of loans and track the status of claims regarding these loans. A claim in this context refers to the process used to close a loan before repayment for reasons such as total permanent disability or death.

1.3. What are the technical elements and/or components of the IT system? Mark all that apply.

☒ Website	☒ Portal	☒ Application
☒ Database	☒ Server	☐ Other (Specify Below)

If you have been directed to "specify below," describe the type of technical elements and/or component:

1.4. Describe the purpose for which the personally identifiable information (PII)[1] is created, collected, used, processed, stored, maintained, disseminated, or disclosed by the IT system. If there is more than one type of individual from whom PII is collected (e.g., grantees, parents, Federal employees, contractors), specify the purpose for each type of individual.

The purpose of the system is to:

- Identify students participating in the HEAL program.
- Compute insurance premiums for federal insurance.
- Monitor the loan status of HEAL recipients, which includes the collection of overdue debts owed under the HEAL program.
- Compile and generate managerial and statistical reports.
- Process claims.

[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 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. OMB Circular A-130, page 33

- Produce an annual report that contains aggregate information.

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

Contractor

1.6. If the IT system is operated by a contractor, describe the contractor's role in operating the system.

☐ N/A

The HOPS contractor supports and enables the continual and efficient operation of HOPS. The HOPS contractor responsibilities include but not limited to the following:

- Monitor/maintain operation and maintenance processes.
- Provide system status reports.
- Create HOPS user accounts.
- Administer the webserver and related applications on the server.

1.7. If the IT system is operated by a contractor, does the contract and other acquisition-related documents include privacy requirements?

Yes

☐ N/A

2. Legal Authorities and Other Requirements

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

2.1. What specific legal authorities permit and regulate the collection and use of data by the IT system? Include name and citation of each authority.

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). The collection of SSNs that are maintained in this system is authorized by 5 U.S.C. 301 and Executive Order 9397, as amended by Executive Order 13478 (November 18, 2008).

System of Records Notice (SORN)

2.2. Has the Department's Privacy Program determined that the PII maintained by the IT system is or will be maintained as part of a Privacy Act system of records? Refer to the "SORN" item in the "Privacy Program Determination" section of the PTA if unsure.

☒ Yes

☐ No

2.3. If yes, provide the full name(s), number(s), and Federal Register citation of the applicable SORN(s) and/or a statement indicating that a new or modified SORN is being prepared.

The SORN, titled "Health Education Assistance Loan," 18-11-20, 83 FR 40264, was published in the Federal Register on August 14, 2018.

Records Management

If you do not know your records schedule, consult with your records liaison, or send an email to RMHelp@ed.gov

2.4. Is there an applicable records retention schedule(s) for the information maintained in the IT system? Note: If no records schedule is in place or you are unsure of the applicable records schedule, reach out to your records liaison or the Records Management Office.

☒ Yes, there is/are approved records retention schedule(s) for the information.
List the schedule(s):

All records are retained and disposed of in accordance with the Department's records schedule, National Archives and Records Administration (NARA) disposition authority DAA-0441-2017-002 ("FSA Health Education Assistance Loan (HEAL) Program Online Processing System (HOPS)"). Records shall be destroyed seven years after cutoff. Cutoff occurs annually, upon final payment or discharge of the loan.

☐ No, there are currently no approved records retention schedules, but there is a proposed schedule or plan to establish a schedule. Explain:

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

☒ Yes

☐ No

3. Information Collection, Maintenance, Use, and/or Disclosure

Collection

3.1. Select the types of PII that are collected, maintained, used, and/or disclosed by the IT system. **Note:** PII includes any information that is linked or linkable to an individual, including business or contact information, information that is publicly accessible elsewhere, and ordinarily non-sensitive information.

Biographical and Contact Information

☒ Name	☒ Date of Birth	☐ Gender or Sex
☐ City, State, or County of Birth	☐ Country of Birth	☒ Home Address
☒ Personal Phone Number	☒ Work Phone Number	☐ Personal Email Address
☐ Work Email Address	☒ Work Address	☐ Personal Fax Number
☐ Work Fax Number	☐ Digital Signature ☐ Hand Signature	☐ Mother's Maiden Name

Other Demographic Information

☒ Citizenship and/or Alien Registration Number (A-Number)	☐ Military Service	☐ Marital Status, Spouse, and/or Child Information (Specify below)
☐ Educational Background/Records	☐ Group/ Organization Membership	☐ Employment Information
☐ Physical Characteristics or Biometrics (Height, Weight, etc.)	☐ Race/Ethnicity	☐ Religion

Identification Numbers

☒ Social Security Number	☐ Truncated/Partial Social Security Number	☐ Driver's License Number

☐ Passport Number	☐ Employee Identification Number	☐ Professional License Number
☐ Credit/Debit Card Number	☐ Bank/Financial Account Number	☐ Personal Device Identifiers/Serial Numbers
☐ License Plate Number	☒ File/Case ID Number	☐ Federal Student Aid Number
☐ Student ID Number	☒ Student Loan Number	☐ Grant Number
☐ Other ID That Can Be Traced to Individual (Specify below)		

Electronic and Miscellaneous Information

☐ Username/User ID	☐ Password	☐ IP Address
☐ MAC Address	☐ Complaint Information (Specify below)	☐ Medical Information (Specify below)
☐ Location Data	☐ Log Data That Can Be Traced to Individual	☐ Photographs of Individuals
☐ Videos of Individuals	☐ Criminal history	☐ Other (Specify below)

If you have been directed to "specify below," describe the PII:

3.2. Select the category of individuals from whom information is collected, maintained, used, or disclosed by the IT system and, if applicable, list what information from Question 3.1 is collected from each. Check all that apply:

☒ Federal Employees

Specify types of information collected from Federal employees: name.

☒ Federal Contractors

Specify types of information collected from Federal contractors: name.

☒ General Public (Any individual not employed by the Department).

Specify categories of the general public (e.g., teachers, students, parents, institution representatives, grantees, State, and local government employees), and the types of information collected from each:[2]

From HEAL servicers about recipients: name, date of birth, home address, work address, home phone number, work phone number, citizenship status, Social Security number (SSN), file/case number, educational status, and student loan number.

3.3. What are the sources of PII collected, maintained, used, or disclosed by the IT system (e.g., individual, school, another agency, commercial sources)?

HOPS obtains the recipient's PII from the HEAL servicers and does not obtain PII directly from individuals.

3.4. How is the PII collected from the stated sources listed in Question 3.3 (e.g., paper form, webpage, database)?

HOPS receives monthly batch files from HEAL servicers via the Student Aid Internet Gateway (SAIG) mailbox. The batch file types received are borrower loan status (BLS) datasets, loan transfer/refinancing (TRAN) datasets, forbearance (FORB) datasets, and litigation (LITIG) datasets, and the following datasets from the HHS Program Support Center (PSC)[3]: the student default report (SDR), claims paid upload, and the Federal Agency Registration (FedReg) dataset. These datasets are then loaded and processed through HOPS.

3.5. Privacy law and policy generally requires agencies to collect or maintain only the minimum amount of PII necessary to accomplish an authorized purpose. For each of the PII elements that are indicated in Question 3.1, please describe why the information is necessary.

[2] For example:
From students: name, email address, phone number.
From institution representatives: name, email address, username, password.
[3] Program Support Center (PSC) is an office within U.S. Health and Human Services (HHS) that performs HEAL Program Debt Collection services.

The PII collected and maintained is the minimum amount required by HOPS in order to process and manage HEAL. HOPS utilizes the PII to uniquely identify individuals that have been provided a HEAL and to track the performance of loans and status of claims regarding these loans. apply for aid under the title IV of the HEA and to track the status of applicants and recipients. Additionally, HOPS is used by loan servicers and HHS to view and update the current status of recipients which requires the use of PII to uniquely identify them.

3.6. Who can access the information maintained in the IT system?

☒ Federal Employees

☒ Federal Contractors

☐ General Public (Any individual not employed by the Department)

3.7. How is the PII validated or confirmed to ensure the integrity or quality of the information (e.g., form restricting, verifying newly collected information matches previously collected information, account verification, periodically requesting system users verify their own information in the system)?

The information provided by the recipients is validated by the HEAL servicer. PII is received from HEAL servicers and is validated against existing PII in the HOPS database.

Information Use for Testing

3.8. Is the PII maintained in the IT system used for internal testing, training, and researching new applications or information systems?

No

3.8.1. If the above answer to question 3.8 is **YES**, are you authorized to use PII when such information is used for internal testing, training, and research?

☐ N/A

No

3.8.2. If the above answer to question 3.8 is **YES,** what controls are in place to minimize the privacy risk and protect the data?

☑ N/A

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

3.9. Does the IT system collect or maintain Social Security numbers (SSNs)?

Yes

3.9.1. If the above answer to question 3.9 is **YES**, cite the authority for collecting or maintaining the SSNs.

☐ N/A

The collection of SSNs that are maintained in this system is authorized by 5 U.S.C. 301 and Executive Order 9397, as amended by Executive Order 13478 (November 18, 2008).

3.9.2. If the above answer to question 3.9 is **YES**, explain the purpose for the collection/maintenance and how the SSNs are used.

☐ N/A

SSNs for recipients of HEAL are maintained by the servicers assigned to the recipient. The SSN is required by program participants to satisfy eligibility, loan servicing and loan status reporting requirements under law and regulations. SSNs are also used to match HEAL recipient records contained in HOPS against records contained in the loan servicers' systems.

3.9.3. If the above answer to question 3.9 is **YES**, specify whether the collection of the SSNs is mandatory or voluntary. What are the consequences for the individual of not providing the SSN, if any?

☐ N/A

The collection of SSNs is mandatory.

3.9.4. If the above answer to question 3.9 is **YES**, specify any alternatives to SSNs that were considered and explain why they were not used.

☐ N/A

Alternatives to using SSNs were considered but determined not to be feasible given the lack of a consistently collected alternative identifier that is capable of performing the same function as the SSN. FSA's internal and external data exchanges rely on SSNs to identify, and track HEAL across different systems within and outside of the Department.

4 Notice

4.1. How does the IT system provide individuals with a privacy notice about the collection, maintenance, use, and disclosure of PII prior to its collection? For example, does the IT system provide a Privacy Act Statement (if applicable) or other privacy notices provided at the point of collection? If a notice is not provided, explain why not.

Since the HEAL program is no longer accepting new applications, recipients still have an opportunity to defer payments or apply for total and permanent disability. Respective forms are located on the Department's website for access by individuals who have a current HEAL. Each of these forms have privacy notices detailing the Department's privacy practices.

4.2. If you, or a partner, maintain a program website that is not hosted on the ed.gov domain and is accessible to the public, does the program website have a webpage privacy policy?

No

4.3. Provide a link to the webpage where the privacy notice referenced in Question 4.1 is posted. If there is no publicly accessible link, provide the text of the privacy notice. Do not include security banners, security notices, Paperwork Reduction Act statements, or other notices not specifically related to privacy.

☑ N/A

- Borrower Deferment Request
- Physician's Certification of Borrower's Total and Permanent Disability

4.4. What opportunities are available for individuals to consent to uses of their PII, decline to provide PII, or opt out of the project? If these options are not available, state why not.

After individuals provide PII to FSA, they do not have the ability to decline to provide the PII or opt out from its use. Opportunities to decline to provide PII or opt out are at the initial point of collection on the HEAL. If an individual declines to provide PII, that will prevent the individual's HEAL from being processed.

4.5. Is the notice referenced in Question 4.1 reviewed and revised when there are changes in the practices, policies, or activities that affect the PII and the privacy risks to ensure that individuals are aware of and, where feasible, can consent to, these changes?

Yes

5. Information Sharing and Disclosures

Internal

5.1. Is PII maintained in the IT system shared internally with any other Department IT system(s) and/or principal offices? If the answer is **NO**, skip to Question 5.4.

No

5.2. Which categories of PII from Question 3.1 are shared and with which Department IT system(s) and/or principal offices?

☑ N/A

5.3. What is the purpose for sharing the specified PII with each Department IT system(s) and/or principal office specified in Question 5.2?

☑ N/A

External

5.4. Is PII maintained in the IT system shared with any external entities (e.g., another agency, grantee, school district, the public)? If the answer is **NO**, skip to Question 6.1.

Yes

5.5. Which categories of PII from Question 3.1 are shared and with whom?

☐ N/A

In accordance with section 709(c)(1) of the Act, the names of HEAL recipients who are in default will be published in the Federal Register on an annual basis. Information posted in the Federal Register consist of name, city, State, and 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.

5.6. What is the purpose for sharing the PII with each external entity specified in Question 5.5?

☐ N/A

The Department publishes this information in order to correctly identify the person in default and to provide relevant information to the authorized recipients of this information, such as State licensing boards and hospitals.

A HEAL Program borrower is included on the list of defaulted borrowers if one of the following applies:

- Has had one or more default claims paid.
- Has been excluded from the Medicare program as a result of his or her HEAL default.
- Has not had the Medicare exclusion stayed, or lifted, by the Office of Inspector General as a result of entering a settlement agreement.

5.7. What are the specific authorities that authorize sharing the PII with the external entities specified in Question 5.5?

☐ N/A

As required by section 709(c)(1) of the Public Health Service Act, the names of Health Education Assistance Loan (HEAL) Program borrowers in default on their loans are published in the Federal Register. This information is made available for use by organizations authorized by the statute.

5.8. Does the IT system maintain an accounting of any disclosures made to an external entity?

☐ N/A

No

5.8.1. If so, is the accounting of disclosures made to external entities available in response to a Privacy Act request?

No

5.9. How is the PII shared with the external entity (e.g., encrypted email, transport layer security (TLS) line)? Specify whether the PII is encrypted in transit and state the encryption method that is used.

☐ N/A

Information is sent to the Office of Federal Register through an encrypted Hypertext Transfer Protocol Secure (HTTPS) session.

5.10 Is the sharing conducted pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with the external entities?

☐ N/A

No

5.11 Does the project allow for the PII to be redisclosed by the external entities or require the external entities to request permission prior to its redisclosure? If so, describe the limitations on redisclosure and how they are documented and enforced.

☐ N/A

No

6. Redress

6.1. What are the procedures that allow individuals to access their own information in the IT system? If there are no such procedures, state why not.

If an individual wishes to access the content of a record in this system of records, he or she should contact the system manager listed on the SORN in question 2.3 with necessary particulars such as name, date of birth, SSN, and any other identifying information requested by the Department while processing the request to distinguish between individuals with the same name. The individual must meet the requirements in 34 CFR 5b.5, including proof of identity.

6.2. What procedures are in place to allow individuals to correct or amend inaccurate or erroneous information?

If an individual wishes to contest the content of their record in the system of records, provide the system manager listed on the SORN in question 2.3 with necessary particulars such as name, date of birth, SSN, and any other identifying information requested by the Department while processing the request to distinguish between individuals with the same name. The individual must also provide a reasonable description of the record, specify the information being contested, the corrective action sought, and the reasons for requesting the correction, along with supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant. Requests by an individual to amend a record must meet the requirements of the regulations in 34 CFR 5b.7.

6.3. How does the program or IT system notify individuals about the procedures for accessing or correcting their information?

The SORN listed in question 2.3 explains the procedures for correcting HEAL recipient information.

7. Safeguards

If you are unsure which safeguards will apply, please consult with your ISSO.

7.1. Does the principal office work with their ISSO to build privacy and security safeguards into the IT system?

Yes

7.2. Is an authorization to operate (ATO) required for the IT system?

Yes

7.2.1. If the answer to Question 7.2 is **YES**, does the IT system have an active ATO?

Yes

7.3. What is the NIST Federal Information Processing Standard 199 security categorization of this IT system?

☐Low

☒Moderate

☐High

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

Access to the system is limited to authorized HEAL program personnel and contractors responsible for administering the HEAL program. Authorized personnel include Department employees and contractors, including financial and fiscal management personnel, computer personnel, and program managers who have responsibilities for implementing the HEAL program.

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), HOPS must receive a signed ATO from a designated FSA official. FISMA controls implemented by HOPS are comprised of a combination of management, operational, and technical controls. All users have a specific role assigned to them approved by the Information System Security Officer (ISSO), are required to read and accept a Rules of Behavior and are required to utilize a complex password and two-factor authentication.

Physical safeguards include the staffing of security guards 24 hours per day, seven days per week, that perform random checks on the physical security of the record storage areas. All sensitive data are encrypted in transit and at rest and access to records is strictly limited to those staff members trained in accordance with the Privacy Act of 1974, as amended.

8. Auditing and Accountability

8.1. How does the ISO assess and ensure that the PII is used in accordance with stated practices in this PIA?

The system owner ensures that the information is maintained and used in accordance with the stated practices in this PIA.

The first method is by completing the Department's risk management framework process to receive an ATO. During the ATO process, the HOPS system owner ensures that National Institute of Standards and Technology (NIST) Special Publication 800-53 controls are implemented. The NIST controls include administrative, technical, and physical controls to ensure that information is used in accordance with approved policies and practices.

The system owner ensures the information is used in accordance with stated practices by confirming that the privacy risks are properly assessed, and the data are secured, ensuring appropriate security and privacy controls are implemented to restrict access, and to properly manage and safeguard PII maintained within the system. The system owner participates in all major security and privacy risk briefings, meets regularly with the ISSO, and participates in FSA's Lifecycle Management Methodology (LMM), which addresses security and privacy risks throughout the system's lifecycle.

8.2. How does the ISO continuously monitor and audit the security and privacy controls to ensure effective implementation and safeguarding of PII?

Continuous Diagnostics and Mitigation (CDM) scans are produced on a weekly basis to identify security and privacy vulnerabilities which are reviewed by the system owner, FSA Security Operations Center (SOC), Next Generation Data Center (NGDC) SOC and ISSO. In the review, system owners are notified of any findings that require action. HOPS will also participate in the Ongoing Security Authorization (OSA) program and continuous monitoring program, which provide quarterly reviews of FISMA controls and continuous scans to ensure that security and privacy controls are in place and working properly. HOPS has a regular patching cycle to ensure the system is secured with the most up-to-date capabilities.

The system owner, in coordination with the ISSO and FSA Security Assessment Team (SAT), ensures the information is used in accordance with stated practices by confirming that the privacy risks are properly assessed and that all data are secured, ensuring appropriate security and privacy controls are implemented to restrict access, and properly managing and safeguarding PII maintained within the system. HOPS will also participate in annual assessments and audits as required, to ensure the effective safeguarding of PII.

8.3. What are the specific privacy risks associated with this program or IT system and how are those risks mitigated?

Privacy risks associated with HOPS include unencrypted data being transmitted, lost, stolen, or compromised. Data breaches involving PII, and credentials are potentially hazardous to both individuals and organizations. Individual harm may include identity theft, embarrassment, or financial loss. Organizational harm may include a loss of public trust, legal liability, or remediation costs.

The risks are mitigated by the above-mentioned safeguards, limiting access to only those with a legitimate need to know, utilizing least privilege principles, masking SSNs, encrypting data in transmission, and working closely with the security and privacy staff at the Department. To further mitigate this risk, the following safeguards have been implemented:

- Monthly vulnerability scans
- Annual contingency plan test
- Annual or ongoing security assessments

Risks are also mitigated by regularly updating security patches and device operating software. System patching is performed monthly, and scans are run on the production environment each month in support of the monthly patching cycle. Collecting the minimum PII necessary to achieve the system's purpose also mitigates privacy risks.