US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/21/2016

OPDIV:

ACF

Name:

Head Start Enterprise System

PIA Unique Identifier:
P-8438988-119315

The subject of this PIA is which of the following?
General Support System (GSS)

Identify the Enterprise Performance Lifecycle Phase of the system.
Operations and Maintenance

Is this a FISMA-Reportable system?
Yes

Does the system include a Website or online application available to and for the use of the general public?
Yes

Identify the operator.
Contractor

Is this a new or existing system?
Existing

Does the system have Security Authorization (SA)?
No

Indicate the following reason(s) for updating this PIA.
PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.
Not Applicable

Describe the purpose of the system.
The Head Start Enterprise System (HSES) is designed to serve as a consolidated and comprehensive repository for reliable data about Office of Head Start (OHS) grantees and program operations.

OHS initiated development of HSES in conjunction with the Administration for Children and Families (ACF) Office of Information Services (OIS). The development and deployment of HSES was designed as a phased approach to provide OHS program managers and grantees with centralized access to management information, while minimizing any disruptions to the operation of HS legacy applications and databases. The first phases of development were completed in FY 2007 and FY 2009; additional phases have been scheduled on a yearly basis since the inception under the direction of OHS.

HSES is designed to solve these problems, by providing a single, authoritative repository of up-to-date information about HS grantees and program operations. HSES facilitates a wide range of management information and business intelligence reporting, including real-time monitoring of grantee performance. For example, HSES allows OHS to actively manage program risks, by the timely identification of potential grantee performance, financial management, or reporting problems.

HSES serves as the operational data store for all HS grantee and program operations legacy applications. It is designed to streamline and simplify the integration of existing HS applications, interfaces, and databases through the provision of a range of flexible and efficient integration mechanisms.

Describe the type of information the system will collect, maintain (store), or share.

OHS collects grantee director contact and data required to monitor the program performance of the grant. Grantees are asked to keep their contact data up to date to facilitate communication. This contact data includes names, phone numbers, e-mail addresses, and grantee organization mailing addresses. Additionally, grantees report monthly enrollment data and submit the annual Program Information Report (PIR) and refunding applications through HSES. HSES does not collect information from the public, except for the purpose of granting access to the PIR site. The PIR data is made available to the public, including researchers, by request, after they provide contact data, limited to name, e-mail address, phone number, and organization mailing address, in order to establish an account for that purpose. Grantees include Head Start and Early Head Start child-serving programs, Collaboration Offices often housed within state agencies, and National Training and Technical Assistance Centers. State collaboration grantee directors are provided with reports from HSES that contain names, email addresses and phone numbers of all state collaboration grantee directors, in order to facilitate collaboration efforts.

All system administrators are contractors, but not direct contractors, who login to their individual user accounts, which have role-based privileges. For example, a member of the database administrator group has privileges to administer the database but not the system or network devices. A network administrator has privileges to administer the network devices, but not the system or database. Administrators access the system by first connecting remotely to a VPN, which requires two-factor authentication (Google Authenticator), or using two-factor authentication to access the physical server in the data center, followed by login with individual user name and password. User names and passwords for the administrators are securely stored in the system.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

HSES supports enterprise functions for the Office of Head Start and consolidates data across all OHS applications. OHS collects grantee director and other grantee employee contact information and data required to monitor the program performance of the grant, to facilitate management of the grant throughout various stages of the federal grant lifecycle, to ensure completion of grant funds planning, and to establish and maintain end user accounts.

Grantees are asked to keep their contact data up to date to facilitate communication. This contact data includes names, phone numbers, e-mail addresses, and grantee organization mailing addresses. OHS program specialists verify the accuracy of the contact and other data when preparing Funding Guidance Letters and other periodic communication.

Additionally, grantees report monthly enrollment data and submit the annual Program Information Report (PIR) and refunding applications through HSES. HSES does not collect information from the public, except for the purpose of granting access to the PIR site.

The PIR data is made available to the public, including researchers, by request, after they provide contact data, limited to name, e-mail address, phone number, and mailing address, in order to establish an account for that purpose. Grantees include Head Start and Early Head Start child-serving programs, Collaboration Offices often housed within state agencies, and National Training and Technical Assistance Centers. State collaboration grantee directors are provided with reports from HSES that contain names, email addresses and phone numbers of all state collaboration grantee directors, in order to facilitate collaboration efforts.

Collected data are maintained in HSES permanently or until times that will be identified when a records retention schedule is developed. User name and password credential are collected and storedsecurely in the system.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name

E-Mail Address

Mailing Address

Phone Numbers

User credentials

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Employees

Public Citizens

Business Partner/Contacts (Federal/state/local agencies)

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

The PII in HSES is used to provide information to grantees and for user account setup and administration, which includes the granting of roles and menu/data viewing privileges.

Describe the secondary uses for which the PII will be used.

To assist with planning the Head Start Review by referencing the contact information for employees in the grantee organization who are responsible for different services.

To facilitate the collaboration requirements described in the Head Start Law, 42 U.S. Code § 9837b, by providing the contact information for all state collaboration directors to each collaboration director.

Identify legal authorities governing information use and disclosure specific to the system and program.

42 U.S. Code § 9836a - Standards; monitoring of Head Start agencies and programs, Section (b)(4) of states:

"Confidentiality
(A) In general The Secretary, through regulation, shall ensure the confidentiality of any personally identifiable data, information, and records collected or maintained under this subchapter by the Secretary and any Head Start agency."

Are records on the system retrieved by one or more PII data elements?

No

SORN is In Progress

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

State/Local/Tribal

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

0970-0207 GABI 06/30/19
0970-0427 Program Information 10/31/2017

Is the PII shared with other organizations?

No

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

The HSES system and Help Desk agents request current contact information for OHS notifications and account administration. The individual does not receive a notice about the personal information that will be collected. The PII collected is consistent with the Federal guidance to agencies when establishing user accounts for systems that use e-authentication.

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

HSES has no opt-out option for grantees and it does not collect information from the public, including researchers, except for the purpose of granting access to the PIR site. OHS currently requires the information from grantees for enrollment reporting and funding of grant applications. Members of the public do not need to submit PII to view publicly-available data.

System administrators are not allowed to opt-out of the collection and use of their user credentials, because those credentials are essential parts of a security control required for FISMA compliance.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

Should a major change occur, the Office of Head Start (OHS) privacy policy notice on the Head Start website will be updated. In addition, the System of Record Notice will be updated and posted on the HHS website to inform the public.

System administrators will be notified of major changes by the Information System Security Officer (ISSO) and/or system owner.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

If an individual is concerned about inappropriate use or sharing of PII they can contact OHS directly or report the issue to our OHS Help Desk via phone, fax, or e-mail; or by using the information and methods specified in the “Contact Us” button on the Early Childhood Learning and Knowledge Center (ECLKC), OHS public web-site.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

Program specialists review PII to facilitate work with grantees. These specialists verify the accuracy and relevancy of the contact and other data when preparing Funding Guidance Letters and other periodic communication.

HSES has both primary and secondary servers, so that if the primary servers fail, the secondary servers automatically take over to ensure information is readily available. The system displays a reminder on the Contacts page for Grantee users to review and correct or update their contact information. A message to review and update the contact information is included in the PIR and Center Reset communications each year and in other communications to users throughout the year. A process exists where all email failures for Eblast Communications are reviewed, follow up with Grantees and OHS is performed, and user accounts and contacts are corrected and disabled as appropriate. Data integrity is maintained by disabling access for users no longer associated with a grant, or when the grantee organization fails to retain a grant. Use of the https internet protocol ensures data integrity through the use of encryption when users enter or receive data while using the system.

Identify who will have access to the PII in the system and the reason why they require access.

Users:

Limited read/write access based on role.

Administrators:

Full access to read data and maintain central functions.

Developers:

Used for account setup and administration.

Contractors:

Contractors fulfill roles of System Administrators and Developers.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Help Desk system users are required to have access to PII for their duties in assisting grantees. System administrators are limited to the system owner and the operations team responsible for day-to-day operations of HSES. Grantee directors are given user administration privileges to add and modify accounts for users in their specific program, and are authorized to grant that privilege.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

Access to information, including PII, is managed in HSES by permissions and privileges that are granted on a per individual basis. Users are only allowed to access information that is specific to their responsibilities. Those users' access is further limited to specific areas of responsibilities specific to their jobs. Other users at central office, including contractors having overall access to HSES, are placed in positions of trust and have undergone federal security clearance. All users are required to adhere to all policies, procedures and rules of behavior.

Contractor users are not direct contractors.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

Federal and contractor staffs who access or operate the HSES system are required to complete the annual HHS/ACF security awareness and privacy training program and to read the Rules of Behavior and sign the accompanying acknowledgement.

Contractor users are not direct contractors.

Describe training system users receive (above and beyond general security and privacy awareness training).

Not applicable

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

Grantee contact data is available for as long as the grantee accounts are active. Once the grantee relationship terminates, the account and available system data are locked and inaccessible to the grantee. User log-in and password data files are covered by NARA Records Schedule 812-1; the data will be destroyed when no longer needed for agency/IT administrative purposes. The records retention schedule is being determined for the user contact data and until then, it is retained in the system indefinitely.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

HSES follows the Office of Management and Budget (OMB) and Department requirements, as well as the National Institute of Standards and Technology Special Publication (NIST SP) 800-53 and 800-53A guidance for securing PII. All data is secured on a database that can only be viewed by users with the correct privileges. In the application itself, being able to view or modify data is limited based on roles. Certain menus and data are not shown to those without the proper roles.

Access to the systems is given based on need to know and job responsibilities. Operating system access control functionality is configured to grant or deny access to data based upon 'need to know' roles. Security assessments and audits also verify these controls. Technical controls used include user identification, passwords, firewalls, virtual private networks and intrusion detection systems. Physical controls used include guards, identification badges, fingerprint scanners and closed circuit televisions.

Identify the publicly-available URL:

https://hses.ohs.acf.hhs.gov/pir

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Session Cookies that do not collect PII.

Does the website have any information or pages directed at children under the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

Yes