

# US Department of Health and Human Services

## Privacy Impact Assessment

**Date Signed:**

01/07/2015

**OPDIV:**

ACF

**Name:**

Unaccompanied Alien Children Portal

**PIA Unique Identifier:**

P-9614390-049466

**The subject of this PIA is which of the following?**

Minor Application (stand-alone)

**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?**

No

**Identify the operator.**

Contractor

**Is this a new or existing system?**

New

**Does the system have Security Authorization (SA)?**

No

**Indicate the following reason(s) for updating this PIA.****Describe the purpose of the system.**

Manage information for Unaccompanied Alien Children (UAC)

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

Information on UACs to include name, alien number, case review details to include sponsor, incidents, medical screening, education and travel request information

**Provide an overview of the system and describe the information it will collect, maintain (store), or share,**

System has Oracle back end to store data and a web server hosting UAC application. Personnel from ACF and programs that house UACs are able to enter and retrieve information from a secure web site at <https://www.uacportal.org>

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

Yes

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

Social Security Number

Date of Birth

Name

Photographic Identifiers

Biometric Identifiers

Mother's Maiden Name

E-Mail Address

Mailing Address

Phone Numbers

Medical Notes

Financial Accounts Info

Legal Documents

Education Records

Employment Status

Passport Number

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

Public Citizens

Unaccompanied Alien Children (UACs) and their sponsors

**How many individuals' PII is in the system?**

50,000-99,999

**For what primary purpose is the PII used?**

To document UACs custody with HHS and to process their release to sponsors

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

None

**Describe the function of the SSN.**

UACs do not have SSN. It is an optional field of information for sponsors for checking background information on them

**Cite the legal authority to use the SSN.**

Trafficking Victims Protection Reauthorization Act (TVPR) of 2008 section 235(c)(3)(B)

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

Homeland Security Act (HSA) of 2002 section 462 (b)(1)(J)

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

Yes

**Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.**

ACF Consolidated SORN 2. 09-80-0321

SORN is In Progress

**Identify the sources of PII in the system.****Directly from an individual about whom the information pertains**

In-Persion

Hardcopy

Email

**Government Sources**

Other Federal Entities

**Non-Governmental Sources****Identify the OMB information collection approval number and expiration date**

OMB 0970-0278 valid through 10/31/2014

**Is the PII shared with other organizations?**

Yes

**Identify with whom the PII is shared or disclosed and for what purpose.****Within HHS**

null

**Other Federal Agencies**

Veterans Administration, Department of Homeland Security, Department of Justice

**Private Sector**

Script Care, LLC, pharmacy benefits company that takes care of prescription drugs for the UACs

**Describe any agreements in place that authorizes the information sharing or disclosure.**

Interagency Agreement with the VA. Memorandum of Understanding (MOU) with DOJ.

Statement of Principles with DHS.

**Describe the procedures for accounting for disclosures.**

Requests for information on specific UAC and/or sponsors must follow the ORR UAC Program Operations Manual policy generally requiring the UAC or sponsor to consent to the disclosure. In some instances ORR may share information with another government agency without the need to obtain a UAC or sponsor's consent. All requests are recorded and archived by ORR staff.

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

Sponsors of UAC are initially informed that their information may be disclosed when a Authorization for Release of Information is sent to the sponsor. The sponsor signs the release in order to proceed with the release of the UAC. The release is limited to the purpose of obtaining a background check on the sponsor. Additionally, the Authorization for Release of Records requires the consent of the sponsor and/or UAC if they agree to have that information released, except under circumstances where another government agency requests information on the sponsor and/or UAC, in those situations ORR will use its discretion.

**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 information collection, provide a reason.**

For UAC there is no opt out to collection as they are children in Federal administrative detention. HHS/ORR is required under the HSA of 2002 section 462 to collect and retain information on these UAC. A sponsor who wishes to "opt out" will not be allowed to sponsor a UAC in HHS/ORR custody.

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

There is no process to notify and obtain consent. UAC are detainees in Federal administrative detention their PII is a required collection under the HSA of 2002 section 462. Sponsor information is required to be kept as part of the background check of the sponsor required under the TVPRA of 2008 section 235. Sponsor's file an Authorization for Release of Information explaining that their information is collected by ORR this is the means ORR uses to notify sponsors that information is being stored and give their consent.

**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 inaccurately.**

In the event that an individual believes that their PII has been inappropriately used they may notify HHS/ORR. If the disclosure appears criminal in nature HHS/ORR will refer the issue to the FBI.

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

No process is in place. This is a very basic database used to maintain the information of UAC in Federal custody and their sponsors.

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

Perform duties assigned to them

**Administrators:**

For supervision and controlling access to information.

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

PII is accessible by system users and system administrators. Each system user has read access to all information. A system user is associated with one or more programs. The system user has write access to only the information from programs that are associated with him or her.

System Administrators are authorized to access the system for purpose of troubleshooting and correcting errors in data entry on the request of ORR Program Manager.

**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 is controlled by the Administrator in ORR UAC Portal. The access rights are controlled by the privilege assigned to the user.

**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.**

Personnel working ORR UAC system are made aware of their responsibility to protect data on the server during regular meetings and trainings. Additionally, ORR care provider staff are required to take various confidentiality trainings regarding UAC/sponsor information. HHS employees and on-site contractors are required to take annual security awareness trainings. Other contractors are required to take contractor required security awareness trainings as required by HHS for contract employee staff.

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

Users are trained by ORR before being allowed to use the system and are required to participate in routine contractor required or Federally required information sharing and security awareness trainings.

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

No

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

Records will be maintained indefinitely until a schedule is approved.

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

Management oversight of activities, security awareness and training for users of the system, conduct disaster recovery exercises, separation of duties for personnel administering the system, isolating development test instances of the system.

**Technical controls**

Secure Socket Layer (SSL) for browser to server communication. User authentication (login) and logical access controls, anti-virus software, fire walls, role based access through application. The database is behind a fire wall, with no direct access to it from outside the network. Password complexity requirements for all user accounts. Password clipping levels established to lock accounts that use incorrect password more than 5 times.

**Physical controls**

Server housed in secure facility, climate control, fire alarm, fire extinguishers and Uninterrupted Power Supply (UPS) for servers.