US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/22/2024

OPDIV:

ACF

Name:

Unaccompanied Children Portal

PIA Unique Identifier:

P-9614390-049466

The subject of this PIA is which of the following?

Major Application

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.

Agency

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

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.

Since the last PIA review, UC Portal has migrated the application and the database server to the Amazon Web Services (AWS) General Services System (GSS) environment.

The fields of Preferred Language(s) and Eye Color have been made required fields in UC Portal.

Describe the purpose of the system.

The Unaccompanied Children (UC) Portal is a system of record for the Office of Refugee Resettlement (ORR) under the Administration for Children and Families (ACF), which tracks the data life cycle of unaccompanied minors who were apprehended at the nation's border by Customs and Border Patrol (CBP), and assigned to ORR for custody.

The UC Portal manages all medical (mental and dental health included), educational, and sponsorship information for UC in ORR custody. It also supports interaction with other stakeholders

including the Department of Homeland Security (DHS), Veteran's Affairs (VA), and Point Comfort Underwriters (PCUs), and meets the reporting needs of higher ACF management.

UC Portal also shares pertinent information with the Government Publishing Office (GPO) for the purpose of generating Verification of Release cards for discharged unaccompanied children.

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

The following information is managed in the UC Portal.

For each UC: Full Name, Date of Birth (DoB), Alien Registration Number (A#), Photograph of individual at various ages and/or locations, Biometric Identifiers (Height, Weight, and Eye Color), Medical Notes (examples: vaccinations, medications, doctor visit details), Preferred Language(s) and Portal ID is assigned to each UC.

In addition to the above personally identifiable information (PII), about 2,000+ data elements are collected for the UC, including Country of Birth (City and Neighborhood of Birth), Educational information,Progress Reports, Race, Religion, and Legal Status.

For the Sponsors of each UC: Social Security Number (SSN)
(The collection and storage of SSNs has ceased, the system continues to store SSNs for sponsors that are covered under a previous Family Reunification Packet (FRP) consent form, prior to June 2018), Full Name, Date of Birth, Email Address, Phone Numbers, Mailing Address, Drivers License Number and Passport Number, Financial Account Information, Employment Status (Income, Proof of income, Employer Name, Address, City, State, Zip, and Phone Number), Legal Documents (Legal Status, Tax returns, government identification documents)

In addition to the above personally identifiable information (PII), other pieces of information collected include: Marital Status, Country of Birth, Gender, and Country of Residency.

Once a sponsor receives custody, additional information is collected on the household (meaning other individuals living in the same residence as the sponsor), to include: Full Name, Date of Birth, Gender, Age, Relationship to the UC

For User Accounts: Full Name, Email Address, Phone Number, Fax Number, Mailing Address, Username and password (credentials), Role and Privileges

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

The UC Portal collects, tracks, and stores data on UCs from the point of apprehension (by CBP) to program exit; this is considered the data life cycle. The program provides this data to authorized system users and organizations, including DHS, VA, and PCU.

The Portal manages a large amount of information, including personal information, medical notes, educational information, and sponsorship information. There are four major groups of individuals for which information is collected:

1. UCs – information includes: Name, DoB, A#, Photographs, Biometrics, Medical Notes, Country of Birth, Education Information, Progress Reports, and roughly 2,000 additional data elements
2. Sponsors – information includes: Name, DoB, SSN, Email Address, Driver's License Number, Passport Number, Phone Number(s), Mailing Address, Financial Account information, Employment

status and income information, Legal Documents, Marital Status, Gender, Country of Residency, and additional data elements
3. Sponsor's Household – information includes: Names, DoBs, Gender, Age, and Relationship to UC
4. System Users – information includes: Name, Email Address, Phone Number, Fax Number, Mailing Address, Username, Password, and Role/Privileges

The system user base consists of federal employees and direct contractors at ACF, approved housing programs for UCs, child advocates, legal services teams, federal field specialists (FFS), CBP, and Immigration and Customs Enforcement (ICE).

UC information is shared with Veterans Affairs (VA), data fields are shared with VA once every day. A comma separated value (CSV) file is copied to a Secure File Transfer Protocol (SFTP) server provided by VA. UC information is also shared with Point Comfort Underwriters (PCU). The CSV file is copied to a PCU-provided SFTP server. UC additionally shares referral information and placement decision information with the CBP United Immigration Platform (UIP) system.

All data contained in the UC Portal is considered temporary and is broken into 2 record groups with differing retention and disposal instructions. The 2 record groups include 'Case Files on the UC, Sponsor, and Sponsor household maintained by the Portal' and 'System User Accounts', including related profile information.

Information that is temporarily shared with GPO, as needed, for purposes of generating a Verification of Release Card includes Name, Preferred Language(s), A #, DoB, Country of Birth, Eye Color, Gender, Address, and Photograph. GPO stores this information only temporarily and permanently destroys it after generating the relevant Verification of Release Card.

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

Driver's License Number

Biometric Identifiers

E-Mail Address

Mailing Address

Phone Numbers

Medical Notes

Financial Accounts Info

Legal Documents

Education Records

Employment Status

Passport Number

User Credentials

Alien Registration Number (A#); Religion; Legal Status

Marital Status; Age; City and Neighborhood of Birth

Gender; Country of Residence; Country of Birth

Progress Reports; Fax Number; Portal ID; Race; Portal ID

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

Employees

Public Citizens

Unaccompanied Children (UC)

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The primary purpose of the PII is to accurately track all UCs in order to make informed decisions about their care.

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

The secondary uses of PII include creating user accounts and the evaluation and approval of Sponsors.

Describe the function of the SSN.

The SSN is collected on any Sponsor who applies for custody and is used as the unique identifier.

Cite the legal authority to use the SSN.

Trafficking Victims Protection Reauthorization Act (TVPRA) 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); Flores Settlement Agreement, No. 85-4544-RJK (Px)(C.D. Cal. Jan. 17, 1997)

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.

ORR Refugee Arrivals Data Systems 09-80-0325

ORR Division of Children's Services Records 09-80-0321

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Email

Government Sources

Other Federal Entities

Non-Governmental Sources

Public

Identify the OMB information collection approval number and expiration date

Administration and Oversight of the Unaccompanied Children Program OMB 0970-0547, valid through 05/31/2025
Release of Unaccompanied Children from ORR Custody OMB 0970-0552, valid through 05/31/2025

Services Provided to Unaccompanied Children OMB 0970-0553, valid through 04/30/2025
Placement and Transfer of Unaccompanied Children into ORR Care Provider Facilities OMB 0970-0554, valid through 06/30/2026

Initial Medical Exam Form and Initial Dental Exam Form - OMB 0970-0466, valid through 12/31/2023

Health Assessment Form, Public Health Investigation Form: Non-TB Illness, and Public Health Investigation Form: Active TB OMB 0970-0509, valid through 12/31/2023

Serious Medical Procedure (SMR) Request Form OMB 0970-0561, valid through 02/29/2024

Is the PII shared with other organizations?

Yes

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

Within HHS

Office of the Chief Information Officer (OCIO) HHS CARES

Other Federal Agencies

PII is shared with: Veterans Administration (VA) for provisioning medical benefits, Department of Homeland Security (DHS) receives the A# when a change is made to a UCs status, and Department of Justice (DoJ) to meet statutory requirements concerning their immigration and/or court status.

Private Sector

PII is shared with: Point Comfort Underwriters (PCU) for the provisioning of pharmacy benefits to the UCs

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

The following agreements are in place to authorize the information sharing mentioned above:
Interagency Agreement (IAA) with the VA;
Memorandum of Understanding (MOU) with the DOJ; Statement of Principles with the DHS;
MOU with CBP;
MOU with PCUs to adjudicate medical services provisioned to UC and process all treatment authorization requests for medical services;
MOA with California Department of Social Services to provide aggregate data (no PII or PHI) on UC discharged to sponsors in California to facilitate provision of services to UC.
Information Sharing Agreement - Office of the Chief Information Officer (OCIO) HHS Coronavirus Aid, Relief, and Economic Security (CARES)

Describe the procedures for accounting for disclosures.

Requests for information on a specific UC and/or sponsor must follow the ORR UC Program Operations Manual policy generally requiring the UC or sponsor to consent to the disclosure. In some instances, ORR may share information with another government agency without the need to obtain a UC 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.

UCs are administrative detainees and are provided a general notice by their care provider that the information they provide is used for care and services. They are not specifically informed of where their data is kept.

Sponsors of UCs are provided an information packet that informs them that their PII data will be collected and used in the decision-making process.

All users of the system are made aware that their PII is collected as part of the user account registration process.

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.

For UCs, there is no opt-out to the collection and use of their PII 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 UC.

A sponsor who wishes to "opt-out" will not be allowed to apply or serve as a sponsor for an UC in HHS/ORR custody.
A user who wishes to "opt-out" will not be granted a system account, but this may not be an option if the user is required to have access based on their job duties.

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 from UCs when a major system change is going to occur as they are children in Federal administrative detention and their PII is a required collection under the HSA of 2002, section 462.
There is no process to notify sponsors of major system changes to the UC Portal. Sponsor information is required for the background checks which are a requirement of the TVPRA of 2008, section 235. At the time of application, sponsors are walked through a Family Reunification Packet (FRP) by their Case Manager which outlines all sponsorship requirements and provides notification of the type of PII that will be collected and stored. Consent is inferred by a sponsor’s decision to apply.
All users of the UC Portal are notified of any system modifications (major or routine) through an email listserv as well as notices that are placed on the home page prior to the change occurring.

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.

In the event that an individual believes their PII has been inappropriately obtained, used, disclosed, or that it is inaccurate, that individual can contact ORR who will evaluate the issue on a case by case basis. Points of Contact (POCs) are listed on the UC Portal home page and there is also a portal helpdesk available. If it is determined by the helpdesk staff that this is an issue of unauthorized obtainment, use, or disclosure, then this will be reported to the ORR staff who will notify the ACF Chief Information Security Officer (CISO) and the ACF Incident Response Team (IRT). The ACF IRT will follow standard operating procedures for handling a privacy incident that involves a breach of PII. If it is determined by the helpdesk staff that this is an issue of inaccuracy in the PII, then the following options are available: Changes to most PII about an UC can be directly handled by the Program staff where the UC is residing or being served and the helpdesk staff can assist in contacting the appropriate staff member.
A change to the A# of any UC must be handled by an ACF/ORR administrator.

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

Data Availability is made possible by making a copy of the production database on a daily basis and storing the copy on a tape drive for backup and potential restore situations.

Data Integrity is maintained by limiting the number of users who have write capability, this is achieved by using role-based access. Roles are separated by Program and by User Type within the system.

Data Relevancy: The relevancy of the data is maintained by following the specific retention and destruction schedules for the 2 data groups (Case Files and User Accounts).

Data Accuracy: The accuracy of data is measured and audited periodically. ORR has a robust monitoring protocol which requires a biennial on-site monitoring schedule. There are also federal project officers, field specialists, and direct contractor staff that monitor and audit facility adherence to ORR data and program requirements on a weekly basis.

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

Users:

Users require access to PII in order to complete day-to-day job duties; users receive read access to all data but must be assigned a role for a specific program in order to edit data. Users are made up of federal staff and direct and non-direct contractors.

Administrators:

Administrators require access to PII in order to conduct monitoring and controlling activities, specifically around user access. Only users in the ORR Administrators role have the ability to edit the A# for a specific record.

Contractors:

Direct contractors serve in the role of help desk staff who act in a limited administrator capacity to resolve case specific issues. Direct and non-direct contractors who work at program and facility locations make up some of the users of the portal.

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

General system users, consisting of employees and direct and indirect contractors that work in the ORR UC program, have access to PII in read-only mode across the system in order to fulfill their job duties. There are roles which can be assigned to general system users that grant write-access to specific programs with an approved project officer request. Only system administrators have the ability to assign and modify access privileges for system users. Project Officers also determine which individuals are granted system administrator access. In addition to controlling user roles, system administrators have write-access to all PII for the purpose of troubleshooting and data entry; however, corrections to data must be approved by the ORR Program Manager first.

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.

All system users have read access to PII across the UC Portal while access to modify PII is restricted based on the role assigned to each user. The roles are configured by program so that if a system user only works with one program, he/she will receive the role that allows access to UC PII within that program only. But if the system user works on three programs, for example, they will be assigned three different roles to match each program they work on. Only system administrators have the ability to assign and remove roles from a system user’s account and that action requires an approval from the user’s project officer.

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.

All ACF employees and direct contractors are required to complete the Annual ACF Security & Privacy Awareness training.

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

There is no additional formal training provided by ORR, however, all personnel working with the system are made aware of their responsibility to protect data during regular meetings. System users are trained in an ad-hoc manner by ORR subject matter experts prior to using the system. ORR care provider staff take confidentiality trainings regarding the PII of UCs and Sponsors. There are User Guides posted within the system and can be accessed by any user. In the future, ORR is planning to implement a requirement for users to acknowledge specific ORR policy and regulations prior to being granted access to the system.

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.

The data in the UC Portal is broken into 2 record groups that have specific retention and destruction schedules approved by the National Archives and Records Administration (NARA).
Case Files on UCs, including Sponsor and Sponsor Household information, maintained within the UC Portal are destroyed 5 years from the cutoff date but are authorized for longer retention if business justification is provided. The cutoff date is the end of the Fiscal Year in which the UC is released from ORR program custody. The disposition authority number is DAA-0292-2019-0009
System User accounts and related profile information are destroyed 6 years after the user account is terminated but are authorized for longer retention if business justification is provided. This retention and destruction requirement is outlined in the General Records Schedule (GRS) 3.2, Item 031.

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

UC Portal security controls for protecting PII are inherited from the hosting platform AWS, inherited from ACF, as well as system specific.

Physical controls inherited from AWS include nondescript facilities with security staffing controlling along the perimeter and various building ingress points, video surveillance, intrusion detection systems, fire detection and suppression, uninterruptable power supply (UPS), and climate control.
At ACF, all individuals accessing an ACF building require two-factor authentication. Visitors and indirect contractors at ACF buildings are required to sign-in with building security and maintain an escort for the extent of their time in the building.

Administrative controls implemented by ACF and UC Portal include management oversight of activities, system administration separation of duties, security and privacy awareness training, and a signed HHS and UC Portal Rules of Behavior requirement for all users (federal staff, direct, and indirect contractors).

Technical controls provided by AWS and managed by ACF OCIO include role-based access, user identification, passwords, firewalls, an Intrusion Detection System, anti-virus software, Transport Layer Security (TLS) for browser to server communication; UC Portal's database is located behind a firewall with no direct access from the outside network.
Password complexity requirements for all user accounts include a minimum length of 8 characters; at least one upper and lower case character, one number, and one special character; last 10 passwords cannot be repeated; and password clipping levels are established to lock accounts that use incorrect password more than 5 times.

Note: web address is a hyperlink.