US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

10/25/2021

OPDIV:

ACF

Name:

Child Care Automated Reporting System

PIA Unique Identifier:

P-4343049-751630

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.

Contractor

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

Date of Security Authorization

9/23/2021

Describe the purpose of the system.

Child Care Automated Reporting System (CARS) collects, stores and reports case level child care data (ACF-801 instrument), aggregate child care data (ACF-800 and ACF-700 instruments), and grantee plan data for administering block grant programs (ACF-118, ACF-118a, ACF-218). This data is reported by all 50 States, 5 Territories, the District of Columbia, and over 260 Federally recognized Tribes, all of which receive Child Care and Development Fund (CCDF) block grants. The Office of Child Care uses this data for the Report to Congress, Government Performance and Results Act (GPRA) reporting, and other departmental reporting purposes.

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

A wide range of childcare data is collected from states, territories, and tribes, such as demographic characteristics of the families and children served. Data collection forms, definitions, and standards can be found on the Office of Child Care (OCC) website.

CARS collects user credentials for approved users accessing CARS to submit data, name, email and phone number of points of contacts at the state level who are submitting the data, and data related to the following approvedOffice of Management and Budget (OMB) forms:

1) ACF-700: Annual aggregate report on families and children served, including number of families, number of and children receiving services by age and by reason of care, average number of monthly hours in care, subsidy amount paid, and number of children served by payment type.

2) ACF- 800: Annual aggregate report on families and children served during the fiscal year, including number of families and children, number of child fatalities, CCDF eligible children receiving public pre-K services, payment methods, provider information, consumer education, pooling factor, and number of families, children and providers funded with CARES Act dollars.

3) ACF-118: Information about how the Lead Agency administers the CCDF program, including information such as CCDF leadership, stable financial assistance to families, equal access to high quality childcare, health and safety standards, and program integrity and accountability.

4) ACF-118a: Information about how the Tribal Lead Agencies administer the CCDF childcare program, including information such as CCDF leadership, eligibility, financial assistance to families, health and safety standards, and qualified and effective childcare workforce.

5) ACF-801: Case level characteristics of families and children receiving services during the month and the providers that serve them. Example data include, state generated case identifier, Federal Information Processing Series (FIPS) code, family zip code, reason for care, co-payment, monthly income, homeless status, family zip code, military service, language spoken at home, race/ethnicity, type of care, monthly subsidy amount, federal employment identification number (FEIN), provider state ID, Quality Rating Information System (QRIS) participation and rating, provider zip code, inspection date.

6) ACF-218: Annual Quality Progress Report (QPR) which collects information from states and territories to describe investments to increase access to high quality childcare for children from birth to age 13. It tracks progress toward meeting state and territory benchmarks for improvement of childcare quality as specified in the CCDF Plan.

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

System collects aggregate and case level data (including SSNs prior to Oct. 2015) on families and children served through the Child Care and Development Fund (CCDF). The data collected includes user credentials for approved users to access the system, name, email, and phone number of the points of contacts at the state/territory and tribal level who are submitting the data, demographic characteristics of the families, such as state generated case ids, income and family size, demographic characteristics of children served, such as month and year of birth (used to calculate the age of a child) and race/ethnicity, and childcare setting information, such as hours, subsidy and type of care.

The information is collected in an electronic format from all CCDF lead agencies (as required by Child Care and Development Block Grant Act, 42 U.S.C. 9858 et seq., 45 CFR 98.71(a)(13)) in the states, the District of Columbia, territories (including Puerto Rico, American Samoa, Guam, Northern Marianna Islands, and the US Virgin Islands), and Tribes. The CCDF State/Territory lead agencies are responsible for completing the ACF-801, ACF-800, ACF-118 and ACF-218 forms. The Tribal lead agencies are responsible for completing the ACF-700 and ACF-118a forms.

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
Name
E-mail Address
Phone Numbers
Military Status

SSNs for records prior to October 2015

Other: Health Insurance Claim (HIC) number, Employee Identification Numbers (EIN), Taxpayer

State generated case IDs; User Credentials; name, email and phone number is collected for state points of contact who submit the required federal report (and not related to families, children and providers participating in program)
Month and year of birth - do not collect date of birth

User credentials; ethnicity/race

Federal Employment Identification Number (FEIN)"

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

Employees
Public Citizens

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

Records prior to October 2015 contained SSNs. This PII is used to uniquely identify case records.

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

Not Applicable - there are no secondary uses of PII in the system

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

Child Care and Development Block Grant (CCDBG) Act, 42 U.S.C. 9858 et seq., 45 CFR 98.71(a)(13).

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.

SORN: 09-80-0371 OCC Federal Child Care Monthly Case Records published in the Federal

Identify the sources of PII in the system.

Government Sources: Within the OpDiv, State/Local/Tribal, and Other Federal Entities
Non-governmental Sources: Members of the Public

Identify the OMB information collection approval number and expiration date

ACF-801: 0970-0167, Expires: 02/28/2022
ACF-118: 0970-0114, Expires: 02/29/2024
ACF-118a: 0970-0198, Expires: 06/30/2022
ACF-800: 0970-0150, Expires: 2/28/2022
ACF-700: 0970-0430, Expires: 01/31/2023
ACF-218: 0970-0517, Expires: 9/30/2021

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 Assistant Secretary for Planning and Evaluation for research purposes.
Other Federal Agency/Agencies: Census Bureau for research purposes

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

Memorandum of Understanding between the U.S. Census Bureau and U.S. Department of Health and Human Services, Agreement No. 0094-FY16-NFE-0068.000

Describe the procedures for accounting for disclosures.

OCC tracks active MOUs for information sharing and ensures any data shared is in agreement.

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

State and Territory CCDF lead agencies collect the personal information directly from the individuals receiving childcare subsidies. These CCDF lead agencies report data to the CARS based on established data reporting processes. CCDF lead agencies are responsible to notify individuals that their personal information will be collected.

System users provide their user credentials in order to access CARS and/or perform administrative duties and they agree to share their personal information when they request a user account. A notification banner will be in place on login to notify them that their personal information will be collected.

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 option to object to the information collection, provide a reason.

Collection of individuals PII is the responsibility of the CCDF lead agencies. Individuals cannot opt out of the reporting of their information to CARS.

System users and administrators provide their user credentials in order to access CARS and/or perform administrative duties, and they agree to share their personal information when they request a user account. There is no opt-out of the collection or use of their PII. If requested, the user will not be issued a user credential.

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

Collection of individuals PII is the responsibility of the CCDF lead agencies. Individuals cannot opt out of the reporting of their information to CARS.

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.

CARS contains data reported by CCDF lead agencies (states/territories/tribes). It is the responsibility of the CCDF lead agencies to resolve an individual's concerns when they believe that their PII has been inappropriately obtained, used, or disclosed.

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

Using the concept of least privilege, basic user access and elevated privilege access is controlled via role-based access controls by user type and by each system.

Integrity: Data integrity of the PII collected is maintained by restricting edit privileges to those users who have been approved by the System Owner. Privileges are set to control access by user type. All user account requests to add, remove, or modify must be approved by the System Owner.

Availability: Data availability is partially inherited by the Appian FedRAMP hosting environment, which hosts the CARS application. An Appian Service Level Agreement states that Appian will provide a monthly up-time percentage of at least 99.9%. Additionally, Appian will be taking backups of the system data, including the PII every 8 hours, as described in the Business Impact Assessment (BIA).

Accuracy/Relevancy: As part of continuous monitoring, the Information System Security Officer (ISSO) and Security Lead, in coordination with the System Owner, are responsible for updating all security artifacts for CARS. These updates must be made as changes occur or are at least reviewed annually. PII collected in CARS will be reviewed at least annually. If PII data is found to be inaccurate, it will be updated. The Privacy Officer is responsible for updating the CARS PTA/PIA stored in the system which also contains PII. The ISSO and Security Lead review all system artifacts annually, including the CARS PTA/PIA. So, if any artifacts require changes, the ISSO or Privacy Officer will make those changes. CARS will automatically disable accounts of users who have been inactive for 60 days, ensuring relevancy. Additionally, CARS will follow specific retention and destruction schedules in accordance with NARA disposition authorities.

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

User: Federal Researchers, i.e., linking data with other Federal Programs/Surveys such as Temporary Assistance for Needy Families (TANF), Survey of Income and Program Participation (SIPP), Current Population Survey (CPS), and American Community Survey (ACS).
Administrators: Limited access to set-up databases, migrate legacy data, and Operation and Maintenance.
Contractors: Direct contractors for statistical reporting, and ongoing hosting and Operation and Maintenance.

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

CARS System Owner, ISSO and Security Lead review the established CARS roles to define who has access to PII information. Currently these roles include: System and application administrators. During the annual review of these roles, the System Owner, ISSO and Security Lead either re-validate each individual's access to PII stored in CARS, authorize PII access to new individuals, or remove an individual's access to PII in CARS. Database access is limited to individuals responsible for database maintenance. These individuals use usernames and passwords to login to the system.

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.

The development of user roles in CARS is based on least privilege - allowing for only those actions a user needs to conduct their business in CARS, including accessing PII.

Limited access is accomplished in the following way. Once users successfully login, they are presented with a landing page with options dependent upon their role. Their options may be:

View announcements, tasks, and reminders
Update name, email, and phone number profile information
Access modules for grantees lists

Internal users only
Access modules for ACF forms

External users only
Request user role permissions

Only Regional Office Program Managers, Tribal Grantees/Lead Agency Users, Tribal Lead Agency Certifiers, State/Territory Lead Agency Users, and State/Territory Lead Agency Certifiers can submit requests to update their access to roles and modules

Approve user role permissions requests
Only Regional Office, Central Office approvers, Tribal Lead Agency Certifiers, and State/Territory Lead Agency Certifiers may approve user requests.

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 staff complete annual privacy training as mandated by HHS. Direct Contractors sign a non-disclosure agreement which states that unauthorized disclosures are punishable by pertinent Federal laws. A standard system security notice/banner is in place for all users. OCIO provides annual privacy training to contractor staff.

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

Federal users receive annual IT security and privacy awareness training as mandated by HHS. Direct Contractors receive privacy training by OCIO annually and review their responsibilities in assuring the protection of customer data.

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.

ACF-118, ACF-118a, ACF-218: DAA-GRS-2013-0008-0001, destroy 10 years after cut off, but longer retention is authorized if required for business use.
ACF-801: DAA-0292-2018-0004-0001, destroy 8 years after cut off, but longer retention is authorized if required for business use.
ACF-800: DAA-0292-2018-0004-0002, destroy 8 years after cut off, but longer retention is authorized if required for business use.
ACF-700: DAA-0292-2018-0004-0001, destroy 8 years after cut off, but longer retention is authorized if required for business use.
A Records Management Plan is in place for the child care data, and will be updated to reflect the new database structure.

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

Administrative: PII will only be accessible to users if they have been granted permission to view it. There is also annual security awareness training for all users holding CARS accounts.

Technical: All traffic will be between end users and the authorization boundary will be sent with HTTPS over port 443. Authentication will be provided using OKTA Multi-Factor Authentication. 60-day password change interval, and a maximum failed login attempt of three is enforced by the system. System and application logs will be reviewed and analyzed on a monthly basis using Appian's logging and auditing feature, which provides continuous and real time auditing with alerts for the system. It will be used to track events as specified in NIST 800-53 R4 security control AU-2. Appian utilizes a cloud-based enterprise Anti-virus/Anti-Malware solution.

Physical: The physical controls will all be inherited from the Appian FedRAMP AWS platform and include the following: Restricting physical access to the data center both at the perimeter and at building ingress points through the help of video surveillance, intrusion detection systems, and two rounds of two-factor authentication for each individual accessing a data center floor. Visitors and contractors are required to have ID, sign-in with building security, and be escorted by authorized staff at all times. Additional physical controls include: Fire Detection and Suppression systems; Uninterruptible Power Supply (UPS); Climate and Temperature control; and Preventative maintenance.