

US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/27/2026

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?

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.

There have been four changes in the Child Care Automated Reporting System (CARS) since the last PIA was approved.

Change 1

The Child Care and Development Block Grant (CCDBG) Act allows tribal grantees to use Child Care and Development Fund (CCDF) funds for construction or major renovation of childcare facilities, upon requesting and receiving approval from the Administration for Children and Families (ACF). Regulations at 45 CFR 98.84(b) require Tribes to make requests in accordance with uniform procedures established by the Office of Child Care (OCC). The funds would be set aside from the Tribe's current CCDF allocation, and not additional funds. CARS now has a new module for tribal grantees to submit set-aside requests for construction for a specific fiscal year. Tribal grantees report the point of contact (name, address, phone number, email) for the request, the fiscal year, funds

requested from mandatory or discretionary funding, and the name of the project. Furthermore, the tribal grantees can upload a set-aside request letter.

Change 2

The Sampling Decisions, Assurances, and Fieldwork Preparation Plan (SDAP) form has been migrated from the Online Data Collection System (OLDC) operated by GrantSolutions into CARS. States can now report in CARS the state's plans for sampling cases and conducting case record reviews to meet the requirements of the Error Rate program. Each state creates, submits, and receives approval for its plan prior to drawing the first sample.

Change 3

The ACF-403 Record Review Worksheet (RRW) provides a standardized template for states to assess the case record to evaluate whether eligibility was correctly determined and whether the subsidy payment was made in the correct amount. Each state must customize, submit, and receive approval for its RRW prior to conducting case record reviews. The OCC federal staff now have the capability in CARS to upload previously submitted RRW forms and approvals.

Change 4

With the expiration of the COVID-19 programs, states and territories no longer report American Rescue Plan (ARP) stabilization grant provider level data (ACF-901). CARS retains the previously submitted records.

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), set-construction aside requests, and error rate reporting (SDAP, ACF-403) . 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. 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 approved forms:

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

2) ACF- 800: State annual aggregate report on families and children served during the fiscal year, including number of families and children, number of child fatalities, payment methods, provider information, consumer education, and pooling factor.

3) ACF-118: Information about how the State 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.

4) ACF-118a: Information about how the Tribal Lead Agencies administer the CCDF program,

including information such as CCDF leadership, eligibility, financial assistance to families, and health and safety standards.

5) ACF-801: State case level characteristics of families and children receiving services during the month and the providers who 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, 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, and inspection date.

6) ACF-218: Annual Quality Progress Report (QPR) which collects information from states/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. This data collection expired and under the Paperwork Reduction Act (PRA) process for renewal. CARS retains previously submitted records.

7) ACF-901: Quarterly provider level data describing the number and characteristics of providers receiving ARP stabilization grants. Example data include state generated provider identifier, FEIN, race/ethnicity, date of award, award amount, intended use of grant. This data is no longer collected with the expiration of the COVID-19 programs. CARS retains previously submitted records.

8) Construction set-aside request: Annually, Tribal Lead Agencies can request CCDF mandatory and/or discretionary funding be set-aside for construction. Example data include point of contact (name, email, phone number), fiscal year, CCDF mandatory and/or discretionary amount, and the name of the construction project.

9) SDAP: Every three years, states must report the improper payment rate for their CCDF program. The state lead agencies begin the process by describing their sampling methodology in the CARS SDAP module. Example data include the sample size, sampling frequency and replacement cases, points of contact for conducting the error rate process (name, title), and definition of errors.

10) ACF-403: The tri-annual Record Review Worksheet (RRW) allows states to describe how they will assess the case records they will sample to evaluate whether eligibility was correctly determined and whether the subsidy payment was made in the correct amount. Each state customizes the RRW to reflect the eligibility criteria in their state.

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 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 income, copay, 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, child care setting information, such as hours, subsidy and type of care, and provider information such as provider zip code and last inspection date.

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), 45 CFR 98 Subpart Kand the Payment Integrity Information Act of 2019 (PIIA)) 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, ACF-218, SDAP and ACF-403 forms. The Tribal lead agencies are responsible for completing the ACF-700, ACF-118a forms, and construction set-aside requests.

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

Phone Numbers

Name, email and phone number is collected for state and tribal points of contact who submit the required federal report (and not related to families/children/providers participating in program)

User credentials (user id, name, email, phone #)

Month and year of birth - do NOT collect date of birth

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

Employees

Public Citizens

How many individuals' PII is in the system?

50,000-99,999

For what primary purpose is the PII used?

Name, email and phone number are collected for state and tribal points of contact who submit the required federal report or are conducting the error rate work (and not related to families/children/providers participating in program). Furthermore, user credentials are collected (email, name, phone number) as part of user access management.

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) and 45 CFR 98 Subpart K.

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

No

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

Identify the sources of PII in the system.

Government Sources

Within OpDiv

State/Local/Tribal

Identify the OMB information collection approval number and expiration date

ACF-801: 0970-0167, Expires: 06/30/2028

ACF-118: 0970-0114, Expires: 03/31/2027

ACF-118a: 0970-0198, Expires: 12/31/2027

ACF-800: 0970-0150, Expires: 07/31/2028

ACF-700: 0970-0430, Expires: 03/31/2026

ACF-218: 0970-0517, Expires: 12/31/2024 (undergoing renewal)

SDAP: 0970-0323, Expires: 3/31/2028

ACF-403: 0970-0323, Expires: 3/31/2028

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.

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 for notifying individuals that their personal information will be collected.

System users provide their user credentials 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 no 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 Federal Risk Authorization and Management Program (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.

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, SDAP, ACF-403: 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.

ACF-901: still pending NARA approval. ACF submitted the SF-115 in February 2022. NARA published the records notice in the Federal Register with a comment due date of Aug. 2025. ACF records management staff are following up with NARA on approval.

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 monthly 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 National Institute of Standards and Technology (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 Amazon Web Services (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.