US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/18/2022

OPDIV:

ACF

Name:

Office of Child Care Monitoring System

PIA Unique Identifier:

P-1280388-872853

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.

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.

No changes to the information collected in OCC Monitoring System.

Describe the purpose of the system.

The Office of the Child Care (OCC) Monitoring System is a system to collect evidence (such as policy manuals or interview findings) from States and Territories during monitoring visits to determine State/Territory compliance with the Child Care and Development Fund (CCDF) requirements and to document the findings of the monitoring team. The monitoring team composed of OCC staff and its direct contractor, will enter data prior to, during, and post site visit to document their findings on whether States/Territories comply with CCDF rules. The rules for CCDF compliance are regulatory requirements that States and Territories must adhere to.

The CCDF Reauthorization Regulatory Changes are available at https://www.acf.hhs.gov/sites/default/files/occ/ccdf_tracked_changes_of_existing_regulations.pdf

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

The OCC Monitoring System will contain the following data: Grantee: Name/State or Territory, cohort, monitoring fiscal year, Administration of Children and Families (ACF) region, Lead Agency information (agency name, website, physical and mailing addresses, cohort, next monitoring fiscal year, agency contact information, including work email), CCDF agency information (agency name, website, agency phone number & extension, agency alternate phone number & extension, link to CCDF policy manual, link to CCDF administrator rules, CCDF administrator contact information including work email, CCDF administrator physical and mailing address, CCDF co-administrator contact information, CCDF co-administrator physical and mailing address),
Rules: Rule section number and section name, rule subpart and subpart description, rule number, short description of rule, full description of rule
Monitoring activity: Phase (pre-visit, post-visit, or on-site visit), status (pending or complete), type (monitoring, other), activity date, each rule that is being monitored in this activity, flags (training and technical assistance (T/TA), follow-up, and n/a), method (document review, in-person interview, phone/virtual meeting interview, child care provider visit, stakeholder panel, other), text narrative about this activity
Compliance determination: overall determination status (pending or complete); overall determination date (when complete); each rule being monitored has a determination status (pending, compliant, or not compliant)
Decision: decision and decision date
Event: name, start/end date, region, and state/territory
Task: name, due date, completed date, set alert, assigned user, and state/territory
Announcement: title, body, start date, end date, active status, and audience (global, central office, or grantees)
Resource (such as user guide or training document): title, body, readable filename, and file

The system will also contain user credentials (username and password), roles, and audit logs.

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

The OCC Monitoring System is a system to collect evidence (such as policy manuals or interview findings) from States and Territories during monitoring visits to determine State/Territory compliance with the CCDF requirements and to document the findings of the monitoring team. The monitoring team composed of OCC staff and its direct contractor, will enter data prior to, during, and post site visit to document their findings on whether States/Territories comply with CCDF rules. The rules for CCDF compliance are regulatory requirements that States and Territories must adhere to.

The data will be stored temporarily and destroyed 10 years after final action is taken on file, but longer retention is authorized if required for business use. Reports will be generated from the system and shared with senior leadership.

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

Yes

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

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

How many individuals' PII is in the system?

100-499

For what primary purpose is the PII used?

The PII data is primarily used to create user accounts for system access, and to identify the State and Territory agency officials responsible for implementing the CCDF Block Grant, which are the points of contact for coordination of site visits. This contact information is publicly available at https://www.acf.hhs.gov/occ/resource/state-plans

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 98.90

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

No

Identify the sources of PII in the system.

Identify the OMB information collection approval number and expiration date

Not applicable – OMB Information collection approval number not needed per Office of General Counsel (OGC).

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 agency officials responsible for implementing the CCDF Block Grant provide their business contact information in their application for the CCDF Block Grant. This contact information is publicly available at https://www.acf.hhs.gov/occ/resource/state-plans. State and Territory agency officials notify OCC when the contact information changes through an amendment to their block grant application. PII collection is required when the user requests a user account, therefore a notice is not provided.

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.

System users and administrators provide their user credentials in order to access the system or perform administrative duties, there is no opt-out of the collection or use of their PII. If user does not want to share their business contact information (email, agency), 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.

State and Territory agency officials responsible for implementing the CCDF Block Grant provide their business contact information in their application for the CCDF Block Grant. This contact information is publicly available at https://www.acf.hhs.gov/occ/resource/state-plans. Agency officials who apply for the CCDF block grant cannot opt out from the collection of their business contact information as it is a condition of the grant. The collection of PII is required for the creation of a new user account.

Therefore, users provide consent when creating a user account. Announcements, including any system change(s), appear on the system homepage to notify users. In addition, users are notified via email of any system changes.

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.

After log-in, at the user's discretion, system users and administrators can access their, or the requesting user's, account profile and make changes to the business contact information. State and Territory agency officials responsible for implementing the CCDF Block Grant provide their business contact information in their application for the CCDF Block Grant. This contact information is publicly available at https://www.acf.hhs.gov/occ/resource/state-plans. State and Territory agency officials notify OCC when the contact information changes through an amendment to their block grant application. Users can contact the Monitoring System help desk to resolve any issues or concerns. The phone number and email address for the help desk are both found on the system's homepage. The system will use Visual Studio Team Services (VSTS) for tracking requests for assistance and resolution.

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

After log-in, at the user's discretion, system users and administrators can access their, or the requesting user's, account profile and make changes to the business contact information. State and Territory agency officials responsible for implementing the CCDF Block Grant provide their business contact information in their application for the CCDF Block Grant. This contact information is publicly available at https://www.acf.hhs.gov/occ/resource/state-plans. State and Territory agency officials notify OCC when the contact information changes through an amendment to their block grant application. The Monitoring System will adhere to the established ACF Chief Information Security Officer (OCIO) policy and schedule of backups. The system's availability is handled at the infrastructure level by the hosting platform, Amazon Web Services (AWS). In case of failure, automated processes will move traffic away from the affected area using AWS availability zones. Additionally, the system will validate PII through audit logs tracking updates made to user accounts.

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.

Administrators of the system grant access according to roles to ensure that system users are only granted minimum access to PII information. Database access is limited to those individuals responsible for the maintenance of the database through usernames and passwords.

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.

Administrators of the system will grant access based on roles assigned to the system user. System users are granted only the access necessary to perform their job. Users of the system will only have access to their own user credentials. Administrators of the system will have access to all user credentials. Users will have access to State and Territory agency officials responsible for implementing the CCDF Block Grant contact information. This is publicly available information is located at https://www.acf.hhs.gov/occ/resource/state-plans .

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 direct contractor staff are required to complete annual HHS ACF Cybersecurity Awareness training and sign the HHS Rules of Behavior upon on-boarding. A standardized HHS security notice is also in place on the information system.

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

Direct contractors receive contractor-provided training on their responsibilities in assuring the protection of customer data and are required to sign a non-disclosure agreement (NDA) that states any unauthorized disclosures are punishable by pertinent Federal laws.

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.

Monitoring system data will be deleted in accordance with DAA-GRS-2013-0008-0001 (GRS 1.2) record retention disposition instructions. The data will be stored temporarily and destroyed 10 years after final action is taken on file, but longer retention is authorized if required for business use.

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

Physical Controls are inherited from the hosting platform, AWS and include nondescript facilities, with security staff controlling both the perimeter and various ingress points within the building, video surveillance, intrusion detection systems, fire detection and suppression, uninterruptible power supply (UPS), and climate control; all individuals accessing the building require two-factor authentication a minimum of two times and any visitor or contractor must sign in and be escorted at all times by an authorized individual. Technical controls include role-based access, user Identification, passwords, firewall, intrusion Detection System provided by AWS and managed by ACF OCIO Administrative controls include HHS security training is provided to Federal and in-direct contractor staff, and NDAs are in place for direct contractor staff.