US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/18/2022

OPDIV:

ACF

Name:

National Child Welfare Data Management System (NCWDMS)

PIA Unique Identifier:

P-4469678-376279

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)?

No

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

This effort is to develop a solution to manage a National Child Welfare Data Management System (NCWDMS) for two programs: the Adoption and Foster Care Analysis and Reporting System (AFCARS 2.0) and Title IV-E of the Social Security Act Prevention Program Plan (IV-E PPP) data (as well as build a foundation to support additional data sets in the future) based on standards set forth by Children's Bureau (CB). The goal of this effort is to modernize and replace existing systems to provide a new CB enterprise-wide system to increase the efficiency and effectiveness of the information technology (IT) supporting CB-wide child welfare data management and reporting.

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

NCWDMS will collect three distinct sets of data: Adoption and Foster Care Analysis and Reporting System (AFCARS) data, Family First data, and System User data.

1) AFCARS (205 data elements): Contains information about each child's removal/out of home experience such as location, Date of Birth (DOB), biological parental data, adoption dates, special-

needs and other demographic information.

2) Family First (19 data elements): Contains state level information on prevention plans and the associated, children (demographic information and foster care outcome) and service data (general category of service and costs).

3) System User: User data includes user's names, business phone numbers, business email addresses, for purposes of multi-factor authentication and user management.

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

NCWDMS does not directly collect information on individuals besides system users. States/Territories/Tribes (STTs) (will) upload Foster Care and Adoption data (AFCARS) and Family First Prevention Plan (Family First) data in XML format via an online portal to NCWDMS.

Data is collected and securely uploaded for review by AFCARS and IV-E PPP administrators. All data collected and stored within the NCWDMS is encrypted while in motion and at rest and is maintained and archived in accordance with National Archives and Records Administration (NARA) disposition standards. NCWDMS will reside in the Amazon Web Services (AWS) US East-West public cloud. Uploaded data is encrypted and stored in AWS Simple Storage Service (S3). Once validated and processed, records are encrypted and maintained in the Relational Database Service (RDS).

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

Yes

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

Foster Care Outcome, Service Data, Business Address, User Credentials, Age

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

How many individuals' PII is in the system?

1,000,000 or more

For what primary purpose is the PII used?

The information collected in NCWDMS is collected from AFCARS data and is used for the purpose of analyses and publication of national and state information about children's experience in foster care and/or adoptions. A major product of the AFCARS data include the congressionally mandated Child welfare outcomes report, an annual report that assesses state performance in operating child protection and child welfare programs under titles IV-B and IV-E. AFCARS data, including DOB, is also used by various other Children's Bureau activities to determine compliance with other IV-E report requirements.

Family First data is collected for the data analysis and publication of national and state information about children at risk of entry into foster care and the services provided to them to divert their entry into the foster care system. The data from Family First is used to develop reports to congress. The reports require breaking down the results by demographic information including age.

Profile information for STT and Federal users will be used for authentication, communication, and notification of events.

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

Not Applicable; there is no secondary use of the PII.

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

AFCARS: §479 of the Social Security Act
Family First: Family First Prevention Services Act

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

Per the ACF Paperwork Reduction Act (PRA) Officer, NCWDMS leverages the existing AFCARS and IV-E PPP information collection approvals.

Adoption and Foster Care Analysis and Reporting System (AFCARS)
- OMB #: 0970-0422
- Expiration Date: 5/31/2023

Plan for Foster Care, Prevention and Permanency—Title IV–E
- OMB #: 0970-0433
- Expiration Date: 11/30/2022

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.

Information on children within AFCARS and IV-E PPP is collected by each STT and uploaded to the NCWDMS system for review and reporting. Individuals whom the STTs collect information about are minors and are under the care of the STT. NCWDMS does not have direct involvement in the collection of information by the STT nor the ability to notify the individuals directly.

System Users provide all information that is necessary for their own account creations.

Is the submission of PII by individuals voluntary or mandatory?

Mandatory

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.

Information on children within AFCARS and IV-E PPP is collected by each STT and uploaded to the NCWDMS system. There is no direct opt-out method within NCWDMS.

State/Tribe/Territory users may opt-out of having a user account to access NCWDMS. If they do not provide this information, they will not be granted access to NCWDMS.

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

For Family First data and AFCARS data, CB does not collect this information directly. Information on children within AFCARS and Family First is collected by each STT and uploaded to the NCWDMS system. NCWDMS cannot directly notify individuals whose information is reported via each STT.

If there are major changes to the data collection, notices about the collection are distributed by the CB Deputy Associate Commissioner to
Child Welfare Directors and identified Program Managers at
the state-level.

System Users: NCWDMS system users will be notified through email when major changes and/or data uses change since the notice at the time of original collection disclosures of PII.

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.

NCWDMS is not the source of information collection. CB does not directly collect information on children within AFCARS and Family First. Instead, this information is collected by each STT and uploaded to the NCWDMS system. If an individual has concerns over inappropriate use of their data,

the individual must contact the appropriate agency within the STT.

System Users: NCWDMS system users have the ability to contact system administrators should they believe their PII is being used inappropriately.

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

Integrity: Data integrity of the PII collected within NCWDMS is maintained by restricting edit privileges to only users who have uploaded data or have explicitly been granted rights to modify it. Role-based privileges are set to control access for all NCWDMS users. All user account requests to add, remove, or modify must be approved, and carried out, by a Federal or STT administrative user.

Availability: Data availability is partially inherited by the NCWDMS AWS platform. The AWS Service Level Agreement states that AWS will provide a monthly up-time percentage of at least 99.9%. Additionally, NCWDMS will snapshot all data every 2hrs, as described in the Business Impact Assessment (BIA), to support system Recovery Point Objective (RPO) requirements.

Accuracy/Relevancy: As part of continuous monitoring, the ISSOs / System Owners are responsible for updating all security artifacts for each system. These updates must be made as changes occur or at least annually. So, any PII in the artifacts will be reviewed at least annually. If PII data is found to be inaccurate, it will be updated. The Privacy Officers are responsible for updating the PIA/PTAs stored in the system, which also contain PII. The ISSOs review all system artifacts annually, including the PIA/PTA, so if any changes are needed, the Information System Security Officer (ISSO) or Privacy Officer can make those changes.

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.

Authorized STT users will have the ability to access and upload PII under their control. Federal users will have the ability to review and report on data uploaded by STT users.

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.

Role-based access control will be utilized to ensure each user is granted access to the minimum amount of PII necessary to perform their job. Authorized STT users will only have access to PII which they have created and uploaded to the NCWDMS system. Federal users will have access to review and report on data uploaded by STT users.

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.

ACF Cybersecurity and Privacy Training is required for all users.

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

NCWDMS will also provide system-specific security, awareness, and end user training pertaining specifically to NCWDMS 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.

The contractor (and/or any subcontractor) shall maintain all information in accordance with Executive Order 13556 – Controlled Unclassified Information, NARA records retention policies and schedules, and HHS/ACF policies and shall not dispose of any records unless authorized by HHS/ACF. For the current system, based on discussions with NARA records team, NARA cannot appraise or write schedules for records that do not currently exist. No records will be destroyed until a records schedule is approved.

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

NCWDMS is hosted within the Federal Risk and Authorization Management Program (FedRAMP) Amazon Web Services (AWS) Cloud Platform.

The administrative security controls employed include ensuring that all users holding accounts for the system adhere to ACF and Department policies and procedures around security and privacy and complete annual Security and Privacy awareness training.

The technical controls are shared between the system and the AWS platform. The system provides controls such as multi-factor authentication for all users to include Personal Identity Verification (PIV) login capability and role-based system access to control the amount of PII available to a user. AWS provides infrastructure controls such as secure network access points.

The physical controls will all be inherited by the 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 2 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 are escorted by an authorized staff member at all times. Other physical controls include the following: Fire detection and suppression systems; Uninterruptable Power Supply (UPS); Climate and Temperature control; and Preventative maintenance

All data, including PII, will be encrypted in transit to, and while stored within, the NCWDMS. Only authorized users will have access to upload and manage data which pertains to their specific STT.