US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/22/2024

OPDIV:

ACF

Name:

Child and Family Services Reviews Data Management System

PIA Unique Identifier:

P-8353803-597863

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?

Yes

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.

The PIA is being reviewed and updated as part of an annual review. It was last reviewed and approved by the Administration for Children and Families (ACF) Office of the Chief Information Officer (OCIO) in 2021 as part of the ATO re-authorization of the Child and Family Services Reviews (CFSR) Data Management System (DMS). In the past, the following data changes were made: taxpayer ID captured in the participant database has been removed and the reporting functionality has been modified to no longer include dates of birth. POC has changed and a new OMB control number, which has been reflected in the PIA.

Describe the purpose of the system.

The purpose of the CFSR DMS is to support the Children's Bureau, within ACF, to review state child welfare agencies in achieving positive outcomes for children and families. The goal of the CFSRs is to improve child welfare services and to achieve the outcomes of safety, permanency, and child and family well-being. The CFSR DMS serves as central location for individuals involved in the CFSRs to

access review information, logistical information, state-specific policies, federal policies and guidance related to the review process, training materials related to the case review process, and to access the online data collection and reporting tool used to conduct the actual case reviews. The Children's Bureau implements the CFSRs to review state child and family programs to ensure conformity with the requirements of titles IV-B and IV-E of the Social Security Act. The Department of Health and Human Services (HHS) published a final rule in the Federal Register, which became effective March 27, 2000, to establish the new review system (the CFSRs). States undergo a CFSR once a “Round” (every few years) in collaboration with the Children’s Bureau, however states also use the CFSR DMS regularly throughout the year for their own ongoing Continuous Quality Improvement (CQI) reviews. Round 4 of the CFSRs began in early 2023.

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

The CFSR DMS is comprised of a public facing website and a controlled portion of the system which requires 2-factor authentication to access.

The CFSR Information Portal
The public facing website includes:
1) A resources page and frequently asked questions page, to support the submission of CFSR case reviews and related child welfare policy and legislation.
.
2) Contact page where individuals that visit the site can find contact information for general questions, concerns relating to a specific child welfare case or issues in their state, or specific technical questions about the portal; and
3) log-in page for the controlled portion of the system.

The CFSR Information Portal
Authentication and 2FA required
Upon log-in, authorized users are able to access the CFSR Information Portal. Authorized users consist of state partners, ACF staff, and direct and indirect contractors supporting case reviews and system operation. Each user has a profile that defines their role within the system and what data they can access and what data they act upon such as read-only or edit.

Within the portal, there are several components:

1) The Online Monitoring System (OMS) which supports the state submitting their responses for the Onsite Review Instrument and Instructions and Stakeholder Interview Guide (blank templates of which are all available from the Resources page on the public facing website) and includes the following information: client names, dates of birth (DOB), demographics (race, ethnicity, gender), tribe association, case participant relationships to the primary client, case reason, needs assessments on education, safety, and health well-being.
2) E-Learning Academy (ELA) hosted by Adobe Learning Manager LMS, which provides overviews of the onsite review process (through videos) and more detailed learning coursework and materials on using the OMS to complete the case reviews using mock cases and related mock documents.
3) Participant Database which is accessible only on the contractor internal servers to a very limited number of users, based on role, and includes information collected on the consultant reviewers of the case reviews being submitted and the system users. This information includes name, e-mail address, phone number, role, username, password, account status, mailing address (as needed), and reviewer and auditor qualifications and training history.
4) Document Management System (Huddle) which has limited access based on role and includes an archive for project artifacts, including Statewide Assessments, Final Reports, and Program Improvement Plans.
5) Reporting which provides a visual report of the cases reviewed within the review period at an aggregate level. The visual reports are shown based on the cases and information that an individual

is authorized to see with their role. The Reporting system includes more advanced reports including visualizations, filters, and data indicators which use statistical methods such as Risk Standardized Performance values. Although the data indicators are publicly available data; the visual representations of the data within the Reporting component of the CFSR DMS is only available to authenticated users.

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

The purpose of the CFSR DMS is to support the ACF/Children's Bureau requirement to review state child and family programs and ultimately improve child welfare services to achieve the outcomes of safety, permanency, and child and family well-being. The public facing website provides resource and training material to support all the review instruments that must be submitted by the states, training materials to support the case review process, and child welfare policy and legislation material. The controlled portion of the system, referred to as the portal, includes 5 main components to support the review and audit of the submitted state material and visual reporting of the cases reviewed. All information within the system is maintained temporarily in accordance with approved records schedules: records that exist within the CFSR DMS, specifically in the CFSR Information Portal, OMS, ELA, and Participant Database are maintained temporarily in accordance with disposition authority DAA-0292-2020-003 submitted to NARA in October 2019. These records will be disposed of no sooner than 10 years after the cutoff, which is the end of the fiscal year in which they were collected or created, but are authorized for longer retention as required to support the Children' s Bureau and the CFSRs.

1) OMS/Reporting: Case record reviews (of children and families receiving services from state child welfare agencies), and Interviews (with state child welfare system stakeholders) are both retained within the OMS database until system or project closure; in accordance with the National Archives and Records Administration (NARA) disposition authority DAA-0292-2020-003. Case entities can be the child, siblings, parents, social workers, judges, etc. The following is collected for the child and/or siblings in each case record review; name, age, gender, race, and ethnicity. Names are de-identified. The remaining demographics are aggregated for reporting on how state child welfare agencies around the nation are performing in their service to different populations.

2) Portal/E-Learning Academy (ELA): User profiles of contractor staff, federal staff, and state staff who serve as review team members (user profiles are de-activated if password expires or if person leaves their role, but basic user info is retained in system so that username or email may not be reused on another account), ELA course history (modules completed, test scores, certification status, all retained through current round of reviews after which we retain just summary info in project records). The Portal/ELA does not store any case record review or interview information of children and families served by state child welfare agencies.

3) Huddle (document management system): User profiles of contractor staff only (removed when user leaves project). Documents (Word, PDF, Excel) stored in Huddle are retained until system or project closure; we would follow appropriate plan for closure). We use “Huddle for US, Gov & Healthcare” which is FedRAMP compliant. Huddle does not store any case record review or interview information of children and families served by state child welfare agencies.

4) Participant Database: User profiles of contractor staff, federal staff, and state staff who serve as

review team members Only contractor staff have accounts to access the Participant Database on contractor internal servers (removed when user leaves project). Participant profiles are retained until system or project closure; we would follow appropriate plan for closure. The Participant Database does not store any case record review or interview information of children and families served by state child welfare agencies.

User information for all these applications is captured in the CFSR Information Portal user profile. User name, email address, encrypted password, user role(s), and cell number for two-factor authentication are captured in the Portal user profile. The Portal collects and stores user prof

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

Yes

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

Date of Birth

Name

E-Mail Address

Mailing Address

Phone Numbers

User credentials

Demographics (rage, ethnicity, gender)

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

Employees

Business Partner/Contacts (Federal/state/local agencies)

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

To provide authenticated access to certain portions of the DMS and allow the contractor to provide resource and training material to people involved in the CFSRs.

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

The dates of birth collected within the case file submissions are used to aggregate the data by age for reporting purposes.

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

42 U.S.C. 621 et seq., 42 U.S.C. 670 et seq., 42 U.S.C. 1302.

The 1994 Amendments to the Social Security Act (SSA) authorize the HHS to review State child and family service programs to ensure conformance with the requirements in titles IV-B and IV-E of the SSA. On January 25, 2000, HHS published a final rule in the Federal Register to establish a new approach to reviewing and monitoring State child welfare programs and services. Under the rule, which became effective March 27, 2000, States are reviewed for substantial conformity with certain Federal requirements for child protection, foster care, adoption, family preservation/family support, and independent living services. The ACF/Children’s Bureau administers the review system, which comprises two review components: (1) CFSRs; and (2) title IV-E foster care eligibility reviews.

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.

HHS Department-wide SORN titled “Outside Experts” 09–90–1601

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Hardcopy

Email

Online

Government Sources

Within OpDiv

State/Local/Tribal

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

OMB Control Number: 0970-0214 Expiration Date: 1/31/2025

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.

There is not a formal process for providing notifications to individuals who will have their information collected and maintained within the CFSR DMS. The public website has a system use notification, which includes rules of behavior, and a privacy policy that can be accessed by any site visitor and specifies what information is collected and why.

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.

Individuals required to have a system account in order to participate in CFSRs do not have an opt-out option due to their job responsibilities. Individuals that have PII in the participant database component are required to provide that information as part of their role as a review team member, consultant, or agile staff. If the individual does not wish to provide their information then they will not be contracted into one of those roles.

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

Any change to the purpose or use of the PII collected on system users would be presented to the user as a system notification. The user is then required to acknowledge the notification prior to continued access.

Any changes to the use of review participant PII is communicated to all individuals via email and contact information is shared for any questions or concerns.

Any changes to PII on the case participants is the responsibility of the state to communicate to those individuals. After the states submission, the PII is de-identified prior to further use.

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.

If an individual believes their PII has been inappropriately obtained, used, or disclosed they can

contact the team using any method identified on the Contact Us page of the public website. This information and direction is also available in the privacy policy and system use notification. Any request received that involves a suspected or confirmed misuse of PII will be escalated to the Children's Bureau who will notify the ACF Incident Response Team.
If an individual believes their PII is inaccurate, they can 1) edit their own information, or 2) contact the Child Welfare Reviews Project help desk whose information can be found on the Contact Us page.

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

To ensure the accuracy and integrity of account information, access to view and maintain PII is very limited. Users are granted access to maintain their own PII and a controlled team from the indirect contractor has access to maintain the participant database which is updated when 1) a new individual signs an agreement to serve on case reviews, and 2) when an existing team member departs.

To ensure relevancy of account information, there is a process to automatically disable accounts if management requirements are not adhered to (e.g., change of password within the designated time frame). Additionally, there is an annual review process for all security and PII documentation and this documentation is also reviewed on an ad hoc basis when a change is required.

To ensure availability of the system, the system resides in a FedRAMP (Federal Risk and Authorization Management Program) compliant AWS (Amazon Web Services) cloud with regional failover in place. FedRAMP is a government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

. The cloud-based system is backed up daily.

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

Users:

General users have access to their own PII for account maintenance and to submit the case files. Specific user roles (e.g. case reviewers) have access to the specific reviews they are assigned.

Administrators:

System administrators and help desk staff have access to PII to support operations and maintenance of the CFSR DMS.

Contractors:

Indirect contractors act as system administrators.

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

Access is determined by identifying what information is required for the individual to be able to conduct their job and the specific tasks associated with that. The system employs least privilege in order to limit access and create only the minimal number of users required to access specific PII. Reviews are conducted periodically to update access privileges based on job changes.

We routinely identify the types of PII that are collected and stored in the system, classify the different types of PII in terms of its sensitivity, and limit access to each type of PII to only those roles that must have access in order to perform their job duties. We then routinely review which users have which user roles, and verify the permissions of each user role, to ensure only the minimal number of users required have access to PII in the system. In addition, we routinely review our standardized

procedures, training materials, and required user agreements and confidentiality agreements for adding new system users, as well as our standardized procedures for departing staff. We review these procedures at least annually, as well as whenever system changes are made that affect the type of PII collected or system user roles. Only specific privileged users have access to production data (i.e., although the project no longer employs indirect contractors, in the past indirect contractors did not get production access).

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 system employs least privilege in order to limit access and create only the minimal number of users required to access specific PII. Only those with active "need to know" are granted access to the system.

Access to data in the CFSR DMS is determined by the user's role that is assigned and maintained in the system. Authentication is controlled by centralized authentication via the CFSR Information Portal or in some cases direct access to the specific application. Components such as the Participant Database require stronger authentication since they are available only to JBS personnel. User role assignments are applied when the user is authenticated. Applications that require a higher level of authentication, such as a secure VPN, are also in place where applicable. The onsite review laptops also require authentication to the device. Multi-factor authentication is required to the CFSR Information Portal. Portions of the CFSR DMS do not require authentication and are open access by design.

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 federal users and indirect contractor personnel are required to complete HHS security awareness training annually. Federal users complete HHS provided training as well as the HHS rules of Behavior and the indirect contractor provides training to their employees.

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

All project staff receive specific training on the use and management of the system. All information technology (IT) staff receive additional material on the security components and processes required for the project. Additionally, training on incident response and disaster recovery is provided to privileged users.

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.

Records pertaining to the CFSR, including documents and drafts from the statewide assessments, on-site reviews, program improvement plans, and final reports are maintained temporarily in accordance with the NARA disposition authority DAA-0292-2012-0001-0005. These records are disposed of no sooner than 10 years after the cutoff, which is the end of the fiscal year in which they are collected or created, but are authorized for longer retention as required.

User ETP course history and the participant database are maintained indefinitely while the proposed retention timeline is being reviewed and approved by NARA.

All records supporting system access, including user profiles, are maintained temporarily in accordance with NARA general records schedule 3.2, item 030.

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

The CFSR DMS resides in a FedRAMP (Federal Risk and Authorization Management Program) compliant AWS (Amazon Web Services) cloud with regional failover in place. FedRAMP is a government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

The following controls are in place to secure the information, including the PII, within the system:

Administrative: Required annual awareness training, auditing capabilities, and user acknowledgment of system use requirements at first login and any account re-activation. CFSR DMS employs user account lockout that requires manual unlock by the help desk. All project staff receive specific training on the use and management of the system.

Technical: role-based access control, two-factor authentication required for all users, password requirements (including complexity, expiration, and lockouts after unsuccessful attempts), session timeouts due to inactivity.

The CFSR DMS employs rules for unsuccessful login attempts. On the encrypted laptop used for onsite review, five attempts are allowed for Windows login. On the Portal, 5 unsuccessful attempts within a 2-hour period results in a block. On the Portal, 10 unsuccessful attempts within a 1-hour period results in a lock. To unlock any locked account, users must contact the CFSR DMS Help Desk, and only an admin role can reinstate access. Users must change their password every 90 days. If the password is not changed the account is disabled/expired. The user would need to contact the CFSR DMS Help Desk in order to re-enable the account.

Physical: Regional AWS cloud-based services reside in data centers and are controlled in terms of physical entry and the facility employs environmental controls including maintaining an appropriate temperature, humidity, emergency power, and fire controls. Regional fail-over is also provided for the CFSR DMS.

Identify the publicly-available URL:

https://www.cfsrportal.acf.hhs.gov/

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Session Cookies that do not collect PII.

Does the website have any information or pages directed at children uner the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

No

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

null