US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

04/07/2025

OPDIV:

ACF

Name:

ACF Recipient Experience Portal

PIA Unique Identifier:

P-3619187-596119

The subject of this PIA is which of the following?

Minor Application (stand-alone)

Identify the Enterprise Performance Lifecycle Phase of the system.

Initiation

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.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

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

Describe the purpose of the system.

Current Administration for Children and Families (ACF)ACF grant recipients need to navigate to multiple websites before they’re able to access their grant information. The ACF Recipient Experience Portal will create a secure centralized digital portal for ACF grant recipients. It will streamline access to essential grant information from existing ACF systems, reducing administrative burdens and enhancing the overall grant management recipient experience. ACF grant recipients will use the portal to navigate to their grant information from one location. It will improve communication and coordination across program offices and work to ensure compliance with accurate and timely reporting.

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

The system will collect and maintain name, email, and phone number of ACF grant recipients and a subset of ACF employee points of contact for grant recipients to support effective communications around grants management and compliance activities for ACF grant funding. We are collecting these names, titles, emails, and phone numbers so that ACF can communicate important User’s grant

information and reporting requirements with the correct people and grant deadlines are met and managed more efficiently.

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

The ACF Recipient Experience Portal is strategically positioned within the Office of Grant Management (OGM) ecosystem to serve as a centralized, integrated, and user-friendly access point for grant recipients. The portal promotes data interoperability and leverages single sign-on mechanisms to provide a seamless and efficient experience for users.

The portal will collect grant information weekly from ACF Upstream and the ACF Post-Award Manager (PAM) tool (e.g., grant name, grant amount, grant validity period, due dates).

It will then stor e and maintain the contact information from ACF grant recipients and a subset of ACF staff (e.g., name, role/title, email, phone number) and links to ACF grant systems where recipients can complete grant reporting activities (e.g., system name). Contact information will be temporarily stored each week and then updated/refreshed the following.

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
Due dates
Role / Titles
Grant Name
Grant Amount
Grant Validity period

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

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

How many individuals' PII is in the system?

10,000-49,999

For what primary purpose is the PII used?

The system will collect and display contact information of ACF grant recipients and a subset of ACF staff (whom ACF grant recipients can contact for support with their grants) to enable effective communications around grants management and compliance activities for ACF grant funding.

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

N/A

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

5 USC 301, Departmental regulations

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.

09-90-0025

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Online

Government Sources

Within the OPDIV

Identify the OMB information collection approval number and expiration date

N/A

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.

The site has not yet been developed, but information will be collected using an opt-in model and users will need to consent to provide and share their information. Our estimated timeline for formal go-live is August 2025, with small pilot user testing in March 2025.

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.

The site has not yet been developed, but information will be collected using an opt-in model and users will need to consent to provide and share their information. Our estimated timeline for formal go-live is August 2025, with small pilot user testing in March 2025.

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

Personally Identifiable Information (PII) only pertains to name, email, and phone. A process of notifying and obtaining consent from users during their first log-on attempt after a critical update is currently being developed as the system is not live.

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.

The ACF Recipient Experience Portal team will respond to any concerns raised by a user. Concerns and requests will be triaged to members of the technical team. The technical team will reach out to appropriate personnel to determine the nature of the concern. A Member of the technical team will communicate issues and findings from this analysis to the individual.

Alternatively, Department of Health Human Services (HHS)employees or recipients may contact the HHS Computer Security Incident Response Center (CSIRC) in the event that there is a potential misuse of PII data, at csirc@hhs.gov or 866-646-7514.

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

The site has not yet been developed, details around PII reviews are still being planned.

Integrity

PII attribute read and write permissions are role-based. Role permissions are reviewed by the

development team, CDC Project Owner, and System Security and Privacy Officer during each increment of development.
Reviews ensure that appropriate roles have least privilege permission to access sensitive attributes, protecting the integrity of the data contained in the portal.

Availability
Reports are run incrementally throughout the development lifecycle (pre-production, post-production, and incrementally through operations & maintenance (O&M)).
These reports help in reviewing data elements for anomalies and ensuring data validation governing fields.

Accuracy
Data accuracy is maintained through the use of standard configuration of field values including the use of picklists, date ranges, and minimization of free text where possible.

Relevancy
The design review process includes periodic reviews of PII and Protected Health Information (PHI) when implementing individual attributes in each increment, ensuring that data remains relevant and up to date.

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.

Rationale will be evaluated during the software design process to determine which system identified roles require access to PII. Access and data accessibility, along with role creation/administration processes, will be reviewed with the ISSO in advance of platform administrators creating or assigning roles within the platform.

Administrators
A minimal set of administrators will be able to see PII attributes and developers and other roles not requiring PII visibility will be limited.

Developers
N/A

Contractors
Access to PII will be granted to the Deloitte Operations and Maintenance team members involved in system configurations and data migration tasks that necessitate interaction with PII. All other contractor access to PII will be limited.

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.

PII visibility in the platform will be enforced through role definition and role management. Roles will be evaluated and defined in conjunction with the ACF project manager and associated business offices through creation of user stories and incorporated in 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.

Annual Security and Privacy Awareness training is required for all HHS employees and contractors.

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

Annual Privacy training will be provided.

In addition, Standard Operating Procedures (SOPs) may potentially be used. Notes and emails could also provide training information about the system.

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 will be maintained in accordance with National Archives and Records Administration (NARA) General Records Schedule (GRS). Further processes may be implemented, as the site has not yet been developed.

GRS 2.1, Item 010. Grant and cooperative agreement program management records. Temporary. Destroy 3 years after final action is taken on the file, but longer retention is authorized if required for business use. DAA-GRS-2013-0008-0007

GRS 2.1, Item 020. Grant and cooperative agreement case files. Successful applications. Temporary. Destroy 10 years after final action is taken on file, but longer retention is authorized if required for business use. DAA-GRS-2013-0008-0001
GRS 2.1, Item 021. Grant and cooperative agreement case files. Unsuccessful applications. Temporary. Destroy 3 years after final action is taken on file, but longer retention is authorized if required for business use. DAA-GRS-2013-0008-0006.
GRS 3.2, Item 030 System access records Temporary. Delete when no longer needed for business use (DAA-GRS-2013-0006-0003).

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

The system is in the initiation and planning stages, these controls are still being developed.

Administrative
Administrative controls include a system security plan, contingency plan, regular back up of files and storage of backups off site, role-based security awareness training, least privilege access enforced through roles, separate user and privileged accounts for administrators, policies and procedures in place for retention and destruction of PII, and a corporate incident response team and incident response plans.

Technical
Identification and authentication using unique user IDs, passwords, and smart cards, use of firewalls and intrusion detection/prevention systems, and virus scanning software on all computers. Role based access controls are in place.

Physical
Physical controls are managed by Salesforce, including security guards, ID badges and key card restrictions.

Identify the publicly-available URL:

http://recipients.acf.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.

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