US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

07/09/2025

OPDIV:

ACF

Name:

ACF Zendesk

PIA Unique Identifier:

P-4411008-091860

The subject of this PIA is which of the following?

General Support System (GSS)

Identify the Enterprise Performance Lifecycle Phase of the system.

Implementation

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.

Describe in further detail any changes to the system that have occurred since the last PIA.

Changes to the types of information the system will collect, store, and share.

Describe the purpose of the system.

The ACF Zendesk system is designed to serve as a centralized helpdesk tool that supports multiple workflows essential to the operations of the Administration for Children and Families (ACF). Its primary purpose is to streamline communication, automate processes, and provide efficient issue resolution for both internal and external stakeholders. The system supports the following key functions:

Grantee Support: The system facilitates communication between ACF and its grantees, enabling grantees to submit inquiries, report issues, and request assistance. By automating ticket creation and tracking, the system ensures that grantee concerns are addressed promptly and accurately.

Internal Helpdesk for Data Tools: ACF staff rely on various data tools to perform their duties.

Zendesk provides a structured environment for resolving technical issues related to these tools, ensuring operational continuity.

Agile Tools Support: The system enhances project management and collaboration across teams by providing a platform for tracking tasks, managing workflows, and ensuring transparency in project progress.

Intake Processing: The system automates intake processes, allowing ACF to efficiently collect, organize, and process information submitted by stakeholders, which reduces manual effort and improves data accuracy.

Labor and Employee Relations (LER) Support: The system manages sensitive labor and employee relations issues, including tracking employment-related concerns such as grievances and disputes, ensuring secure handling of employee information including employment status and HHS Employee IDs.

Integrity & Accountability: The system automates case referral and tracking processes related to program integrity matters, which may involve documentation of financial account information and legal documents.

Unaccompanied Children Program Support: The system facilitates comprehensive case management for the Unaccompanied Children Program, supporting:

Child safety verification through collection of biometric and photographic identifiers

Sponsor verification processes requiring identification documents (driver's licenses, passports)

Immigration status tracking using alien numbers

Background screening of potential sponsors and household members, including military status and foreign activities

Management of education records and medical information for proper care coordination

Legal documentation processing for immigration proceedings

System Security Management: The system maintains user credentials and authentication information to ensure secure access to sensitive information across all workflows.

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

The ACF Zendesk system collects, maintains, and shares Personally Identifiable Information (PII) as part of its workflows to support grantee communication and labor and employee relations (LER) processes. The system collects the following types of PII:

Personal Identifiers

The system collects names from grantees and employees to identify individuals submitting tickets or inquiries, which is necessary for tracking and resolving issues specific to each person. For the Unaccompanied Children Program, names are collected from potential sponsors, household members, alternate caregivers, and unaccompanied alien children to uniquely identify individuals within HHS and federal law enforcement systems. Date of birth information is collected from these same individuals to ensure accurate identification and tracking of child safety related matters. Mother's maiden name is also collected to provide an additional layer of identification verification

across systems.

Contact Information

Email addresses are collected from grantees and employees to facilitate communication regarding ticket updates, resolutions, and follow-ups, ensuring timely and accurate responses. For the Unaccompanied Children Program, email addresses help uniquely identify individuals across systems. Phone numbers provide an alternative method of communication for urgent or complex issues when email is insufficient. Mailing addresses are collected from potential sponsors, household members, alternate caregivers, and unaccompanied alien children to verify residence and facilitate written communications when necessary.

Identification Documents and Biometrics

The system collects driver's license numbers and passport numbers from potential sponsors, household members, and alternate caregivers to verify identity and conduct required background checks. Photographic identifiers and biometric identifiers are collected to ensure accurate identification across HHS and federal law enforcement systems, particularly for child safety matters. Alien numbers are collected from employees when relevant to specific labor and employee relations cases, and from individuals in the Unaccompanied Children Program for tracking across immigration systems.

Employment and Background Information

Employment status information is collected from employees as part of the LER workflow, including details such as grade, title, and employment-related issues to ensure accurate handling of personnel matters. For the Unaccompanied Children Program, employment status, military status, and foreign activities information is collected from potential sponsors and household members to assess suitability and ensure child safety. HHS Employee IDs uniquely identify employees within the HHS system for accurate tracking and resolution of personnel matters.

Records and Documentation

The system collects medical records numbers and medical notes for individuals in the Unaccompanied Children Program to ensure appropriate care and tracking of health-related matters. Financial account information is collected when relevant to sponsor verification or benefit determination. Legal documents and education records are maintained to support case management and decision-making processes. All these records help ensure accurate tracking of child safety related matters.

System Security Information

The ACF Zendesk system collects and securely manages user credentials as part of its comprehensive security framework. This includes email addresses (serving as usernames), passwords, and multi-factor authentication (MFA) data to protect the PII maintained in the system.

The system does not collect Social Security Numbers, vehicle identifiers, certificates, device identifiers, or taxpayer IDs.

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

The ACF Zendesk system serves as a centralized helpdesk platform that collects, maintains, and shares information to support various ACF functions. The system collects different types of information based on specific workflow requirements:

Personal Identifiers:

Names are collected from grantees, employees, unaccompanied children, potential sponsors, household members, and alternate caregivers to accurately identify individuals across all workflows.
Dates of birth are collected primarily for the Unaccompanied Children Program to verify age, ensure proper identification, and facilitate appropriate placement and services.
Mother's maiden name is collected for the Unaccompanied Children Program as an additional identifier to ensure accurate matching across systems and verify family relationships.

Contact Information:

Email addresses serve as primary contact methods for all workflows and as usernames for system access.
Phone numbers provide alternative communication channels for urgent matters across all workflows.
Mailing addresses verify residence for potential sponsors in the Unaccompanied Children Program and facilitate written communications when necessary.

Identification Documents and Biometrics:

Driver's license numbers and passport numbers are collected to verify identity of potential sponsors and household members in the Unaccompanied Children Program.
Photographic and biometric identifiers ensure accurate identification of individuals in the Unaccompanied Children Program, particularly for child safety verification.
Alien numbers track immigration status of unaccompanied children and, when relevant, potential sponsors or employees in LER cases involving immigration matters.

Employment and Background Information:

Employment status information supports LER workflows for handling personnel matters and helps assess sponsor suitability in the Unaccompanied Children Program.
HHS Employee IDs uniquely identify employees within the system for accurate tracking of LER cases and helpdesk tickets.
Military status and foreign activities information help assess potential sponsor suitability and security considerations in the Unaccompanied Children Program.

Records and Documentation:

Medical records numbers and medical notes support healthcare coordination for unaccompanied children.
Financial account information is collected when relevant to sponsor verification, benefit determination, or integrity investigations.
Legal documents support case management for immigration proceedings, custody determinations, and other legal matters in the Unaccompanied Children Program.
Education records help ensure appropriate educational placement and services for unaccompanied children.

System Security Information:
User credentials authenticate users and protect access to the sensitive information maintained in the system across all workflows.

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
Photographic Identifiers
Driver's License Number
Biometric Identifiers
Mother's Maiden Name
E-Mail Address
Mailing Address
Phone Numbers
Medical Records Number
Medical Notes
Financial Accounts Info
Legal Documents
Education Records
Military Status
Employment Status
Foreign Activities
Passport Number
Alien Number:
HHS Employee ID
User Credentials

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

Employees
Public Citizens
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 PII is used to support the following: streamline communication, automate processes, and provide efficient issue resolution for both internal and external stakeholders.

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, a Departmental Regulations

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

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

Email

Online

Other

Government Sources

Within OpDiv

Non-Governmental Sources

Public

Media/Internet

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 ACF Zendesk system collects Personally Identifiable Information (PII) as part of its helpdesk workflows to support grantee communication and labor and employee relations (LER) processes. The process for notifying individuals about the collection of their PII is integrated into the helpdesk interaction itself

Grantee Workflow

Grantees are notified that their PII (name, email address, and phone number) is being collected when they submit a ticket or inquiry through the Zendesk platform. The publicly accessible website includes a privacy notice that informs users about the types of information collected, the purpose of collection, and how the information will be used.

The privacy notice is prominently displayed and available in a machine-readable format, ensuring transparency for all users.

LER Workflow

Employees submitting labor and employee relations cases are informed that their PII (name, grade, title, Alien Number, HHS Employee ID, and employment-related issues) is required to process their case. This notification occurs during the intake process, which is typically initiated through internal communication channels (e.g., email, phone, or in-person discussions).

Employees are aware that the information is necessary for resolving employment-related concerns and that it will be handled securely and confidentially.

Reason for No Additional Notification

No additional notification is provided beyond the helpdesk interaction because the collection of PII is inherent to the functionality of the system. The information is voluntarily submitted by individuals as part of their request for assistance or case resolution.

For grantees, the privacy notice on the Zendesk website serves as sufficient notification. For employees, the nature of the LER workflow and internal communication ensures that they understand the purpose of the information collection.

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.

There is no opt-out option, as the collection of PII is necessary for system functionality.

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

There are no plans for a notification process at this time they are still in the development process.

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 system does not have a specific process for resolving concerns about PII, as the information is required to create tickets/cases in Zendesk.

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

The system relies on Zendesk's Federal Risk and Authorization Management Program (FedRAMP)-compliant security measures, including encryption of data at rest and in transit, to protect the integrity of PII. These technical controls ensure that data is not altered or corrupted during storage or transmission.

Availability

Zendesk's cloud-based infrastructure ensures high availability of the system, minimizing downtime and ensuring that PII is accessible to authorized users when needed for resolving tickets or cases.

Accuracy

PII is collected directly from individuals (grantees and employees) during ticket submission or case intake, which reduces the likelihood of inaccuracies. However, there is no formal process to verify or update the accuracy of PII after it is initially collected.

Relevancy

PII is collected specifically for resolving tickets and cases, ensuring that only relevant information is gathered. However, there is no periodic review to confirm that stored PII remains relevant to ongoing workflows or to identify outdated or unnecessary data.

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.

There will be limited administrators that support Zendesk. By default, administrators have access to everything. System users of specific workflows will have access to PII. Other system users will not.

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 ACF Zendesk system employs a combination of administrative, technical, and role-based access controls to ensure that users only access the minimum amount of Personally Identifiable Information (PII) necessary to perform their job functions. These methods are designed to align with

the principle of least privilege, ensuring that access to sensitive information is restricted based on job responsibilities and workflow requirements.

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 authorized personnel are required to complete annual cyber security awareness training (CSAT). This training includes data protection best practices, access control policies, and compliance requirements. The training ensures that personnel understand their responsibilities in safeguarding sensitive information, including PII.

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

N/A

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 are covered by General Record Schedule (GRS 3.2): Information Systems Security Records Item 031

Item 031 System access records: Temporary. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use. DAA-GRS-2013-0006-0004

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

The ACF Zendesk system secures PII through a combination of administrative, technical, and physical controls.

Administrative controls include role-based access control (RBAC) to ensure users only access PII necessary for their job functions, regular access reviews to revoke outdated permissions, annual cybersecurity training for all personnel, and a documented incident response plan to address breaches or unauthorized access.

Technical controls involve encryption of PII both at rest and in transit, multi-factor authentication (MFA) for system access, audit logs to monitor system activity, and adherence to FedRAMP standards, including vulnerability assessments and data segmentation.

Physical controls include hosting the system in Fed Ramp-compliant data centers with restricted access, 24/7 surveillance, and environmental protections, as well as enforcing device security policies such as encryption, secure login protocols, and remote wipe capabilities to protect PII on user devices. These measures collectively ensure the confidentiality, integrity, and availability of PII in compliance with federal privacy and security standards.