US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

12/27/2024

OPDIV:

ACF

Name:

Tyler- Anti-Harassment Program Case Management System (AHPCMS)

PIA Unique Identifier:

P-9488193-448627

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.

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.

The purpose of the Anti-Harassment Program Case Management System (AHPCMS) is to provide a platform that will allow for automated filing of harassment complaints for Administration for Children and Families (ACF) and Health & Human Services (HHS) staff through a web-based portal, and comprehensive administrative management of the resulting harassment cases, together with data management and reporting.

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

The Anti-Harassment system collects and stores information related to Anti-Harassment (AH) cases submitted by ACF employees. Mandatory information collected by the system includes the employee's: first name, last name, and email address. Other information collected may include: physical address, employment status, gender, race, color, national origin, religion, disability type, date of birth/age, management/leadership names, and details about the harassment incident (including type of incident, basis for the harassment allegation; categorization of conduct involved, witnesses and/or other people involved, other details about the harassment behavior, and supporting

documents.

The system does not share any information to other system and organization.

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

The information collected by this the Anti-Harassment system will be related to and controlled by Administration for Children and Families employees submitting an Anti-Harassment case. The mandatory information collected and maintained by the system includes: first name, last name, and email address. Other information that may be collected and maintained includes physical address, (if applicable) gender, race, color, national origin, religion, disability type, date of birth/age, management/leadership names, type of incident, basis for harassment allegation; categorization of conduct involved, witnesses and/or other people involved, other details about the harassment behavior and any This Anti-Harassment application provides a solution for managing every part of harassment cases from intake to resolution while ensuring the interests of all parties are protected. The application is a Commercial Off-the-Shelf (COTS), turnkey product built on Tyler's Application Platform, powered by Entellitrak®. The application features a wide range of out-of-the-box features as well as the capacity to be configured to the specific needs of the client.

Key functions of the Anti-Harassment application include:

Processing cases for physical, sexual, verbal, and visual harassment type complaints

Managing harassment case activity through the entire workflow

Managing correspondence, emails, and documents

The purpose of this system is to allow ACF employees to submit harassment cases and process them.

The following Personal Identifiable Information (PII) is required to submit an Anti-Harassment case:

Field Name

First Name

Last Name

Email Address

There are other optional fields in the AHPCMS system such as:

Phone number

Birth Date

Gender

Race

Color

Nationality

Origin

Disability type (if any)

Religion

Address

Management/Leadership names

Type of incident

Basis for Harassment allegation

Categorization of conduct involved

Witnesses and/or other people involved

Any supporting documents

Other details about the harassment behavior

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
Employment Status
Gender, Race, color, national origin, religion,
disability type, age, Management/Leadership names,
Type of incident, Basis for Harassment allegation,
Categorization of conduct involved,
Witnesses and/or other people involved, Any supporting documents, Other details about the harassment behavior

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

Employees
Vendor/Suppliers/Contractors
If public citizens and/or vendors/Indirect contractors are involved in an incident of harassment –

whether directly or as witnesses – PII relevant to those involved individuals will be collected as well.

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

The primary purpose for use of PII is for documenting the demographic basis that individuals may have for filing workplace harassment complaints, including the follow up to be conducted with the employees involved in harassment complaints.

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

There are no secondary uses for PII outside of managing and resolving harassment complaints. PII may only be used to conduct follow-ups with employees involved in a case. It will not be used for unrelated purposes such as testing, training, or research.

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?

No

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Email

Online

Government Sources

Within 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 process to notify an individual their PII is being collected includes the following:

The Anti-Harassment Program Coordinator informs individuals during the intake process that their personal information will be collected as part of the case management procedure.

Individuals are notified when they login to the system with the notification banner that is displayed on the online portal at the point where PII is collected.

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 currently no documented process or method in place for users to opt-out of the collection or use of their PII. It is the responsibility of the users to handle their PII appropriately and notify the Anti-Harassment Administrators with requests to opt-out.

An aggrieved persons can opt out by filing complaints anonymously. Otherwise, they can also call the Phone: (202) 401-1399 to reach the Anti-Harassment Program to file a complaint anonymously and no personally identifiable information will be collected in the process.

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

Individuals provide their consent at the time they submit an Anti-Harassment (AH) case or when they receive their login credentials, which include a privacy notice, they are required to accept and consent to it before submitting case details. If there are significant changes, such as data breach or new use of information, the ACF Anti-Harassment (AH) Program Coordinator would be tasked with the responsibility of communicating with each impacted individual

Information would also be provided regarding risk mitigation and data recovery as it applies to the specific circumstance of the breach, to the extent that this information is available to ACF and is approved for disclosure.¿ Consent is generally obtained at the time that the individual provides the protected information.

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.

Individuals with concerns about the inappropriate use or disclosure of their PII can contact the AHPCMS system administrators for immediate attention. All concerns will be investigated, and remedial actions will be taken to address issues of data misuse, inaccuracy, or unauthorized access. If needed, the incident will also be escalated to ACF Incident Response Team (acf_irt@acf.hhs.gov) for follow up.

Any cases where there are individual concerns will be handled as they arise by contacting the Anti-Harassment Program manager.

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 process in place for reviews of the PII in the system are not defined, we are currently establishing a method to detail out how we will do reviews for the data.

AHPCMS system currently does not have a formally defined process for periodic reviews of PII to ensure data integrity, availability, accuracy, and relevancy. However, we are in the process of developing and implementing a structured method to detail out how AHPCMS will be doing reviews for the data to establish clear guidelines.

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.

ACF system owner will restrict access to only approved ACF users. The system contains controls which restrict access to PII to approved system users Access to PII within the system is governed by strict access control measures that ensure only authorized users, such as administrator and contractors, have the necessary permissions. These controls are based on the principle of least privilege and role-based access, allowing access only to individuals whose roles require it. Upon the system's Go-Live, no Tyler resources will have access to ACF's systems unless explicitly approved by the ACF System owner.

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.

Access will be granted and controlled by the system administrators who is the system owner so inappropriate users does not have access to PII in the AH system.

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.

Employees using the Anti-Harassment Case Management system have completed Cybersecurity Awareness Training (CSAT). This training ensures that these employees are equipped with the knowledge and skills necessary to manage Personally Identifiable Information (PII) securely and in accordance with federal regulations. The training covers key aspects of data protection, threat awareness, and compliance with privacy policies, thereby ensuring that all staff are fully capable of safeguarding sensitive information within the system.

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

Employees who utilize the Anti-Harassment Case Management System have taken the Tyler User Training module which provides basic information on how to navigate the system and execute the frequently used functions of the software. Each user is also provided with the Tyler Anti-Harassment Case Management User Guide 2.1.0 as a reference text. Each user has also completed CSAT training.

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.

General Record Schedule 2.3 Employee Relations Records Transmittal No. 35, Item 050, Harassment complaint case files. Disposition Temporary. Destroy 7 years after close of case, but longer retention is authorized if required for business use. DAA-GRS-2018-0002-0005

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

Tyler Federal ensures protection of PII by implementing the following.

Administrative Controls:

The system is a cloud-based and administrative controls are handled by ACF. Therefore, ACF implements the following administrative controls on AH: role-based access, users are trained on Cyber Security Awareness Training (CSAT) for proper ways to handle PII and regular audits by the ACF system administrator to prevent unauthorized access or misuse of PII.

Technical Controls:
Electronic storage media including memory devices in computers (hard drives) and any removable / transportable digital memory medium, such as magnetic tape or disk, optical disk or digital memory card, or Transmission media used to exchange information already in electronic storage media are protected in accordance with Tyler Federal Media Protection standards and the technical controls are handled by both ACF and the CSP.

Physical Controls:
Physical control is maintained by the Cloud Service Provider (CSP) hosting AHPCMS, ensuring that server locations are protected with strict physical access controls, surveillance, and restricted entry to authorized personnel only.