US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

01/11/2024

OPDIV:

ACF

Name:

Technical Assistance Website (TAW)

PIA Unique Identifier:

P-5901078-842403

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?

New

Does the system have Security Authorization (SA)?

Yes

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

Describe the purpose of the system.

Technical Assistance Website (TAW) provides guidance and resources for enhancing the effectiveness of Child Care Development Fund (CCDF) programs and improving quality and affordability of childcare services for low-income working parents.

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

TAW provides tribal, state, and territory grantees with guidance and resources for enhancing the effectiveness of CCDF programs and improving quality and affordability of childcare services.

TAW will also collect the users name, email address and credentials when an account is created.

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

The system primarily collects, stores, processes, and transmits data (information types such as resource library records and topical resource pages) in the form of advising and consulting, knowledge dissemination, general purpose data and strategic information, official information

dissemination, social services, and customer services information. It supports all grantees and stakeholders of the Office of Child Care. System users consuming this information are public (not authenticated). System users creating and reviewing this information are authenticated.

TAW will also collect the users name, email address and credentials when an account is created.

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
User credentials

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?

500-4,999

For what primary purpose is the PII used?

Information is retained to support user accounts, and for role-based access to components accessed with login. Also, information is used for the system to send emails to users, and for authenticated users to identify other users who are part of their working group or workflow process.

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

Not Applicable - there are no secondary uses of PII in the system.

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

Child Care and Development Block Grant (CCDBG) Act, 42 U.S.C. 9858 et seq.

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

No

Identify the sources of PII in the system.

Government Sources
Within OpDiv
State/Local/Tribal

Identify the OMB information collection approval number and expiration date

Not Applicable, because the primary purpose for which the PII is used (user account creation) does not require Paperwork Reduction Act (PRA) approval.

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.

TAW does not collect PII data from the general public for this public-facing website. However, direct contractors who maintain the content on the website are required to have login credentials in order to perform their Content Management duties. The direct contractor user sends an account setup

request -- which includes their First Name, Last Name, and business email address -- to the Resource Desk (OCCIT@icf.com). During an employee's onboarding process, a user's supervisor may provide the user's First Name, Last Name, and business email address as part of an account setup request on behalf of the user. When the user account is created, the Resource Desk sends an email to the user notifying them of the new account, credentials, and system URL. The system automatically sends an email to the user notifying them of the new account and specifying their user ID (either First Name Last Name or business email) and initial login instructions. After accounts are created and credentials are communicated to users, they use their user credentials in order to access the system. The following notification banner is in place on the login page to notify users about how the information system's data may be stored and used:

"…By using this information system, you understand and consent to the following:

You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, and for any lawful Government purpose, the Government may monitor, intercept, and search and seize any communication or data transiting or stored on this information system.
Any communication or data transiting or stored on this information system may be disclosed or used for any lawful Government purpose."

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.

If authenticated users (direct contractor personnel) who use the system as part of their job choose to end their employment, their account is disabled and the use of their PII in the system is ended as soon as their employment terminates. Authenticated users who have voluntarily provided their PII in order to request a user account may subsequently request that their account be disabled. A user's PII is no longer used once their account is disabled.

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

Each time that a direct contractor user logs onto the system, the notification banner displays at login to notify them of the current data storage and data uses. If any changes are implemented, such as disclosure practices or data usage, the Lead Developer sends each affected user an explanatory email. System users provide their user credentials in order to access the system, and a notification banner is in place on login to notify them and obtain consent (via the user clicking a link stating "I agree to the terms of the User Agreement") before they continue to access the system.

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.

System users can contact the Resource Desk (OCCIT@icf.com) to request changes to user ID and password. Also, users may contact the Resource Desk (OCCIT@icf.com) with any concerns about PII usage, which are then addressed by Resource Desk personnel.

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

Authenticated system users who have not logged in for 60 days have their accounts inactivated automatically by the system. Inactivated accounts are reviewed at regular intervals to determine if those user accounts should be modified or deleted. System tests also ensure that PII is only available to authorized individuals in association with their assigned role. Authenticated users can request modification to their account's First Name, Last Name, or business email.

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.

Requirements specifications related to system roles identify entities with access to PII information. The product owner and security lead review the roles to determine who has access to PII. These roles include System Administrator, Child Care Technical Assistance Network (CCTAN) Author, CCTAN Reviewer, CCTAN Publisher. Database access is limited to individuals responsible for database maintenance. These roles include Acquia Tech Lead, System Administrator.

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.

Requirements specifications identified entities with access to PII information. Development of these user roles was based on least privilege access principles.

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 personnel, including both direct contractors and government personnel, are required to participate in the ACF annual security compliance training and privacy training. Additionally, personnel with System Administrator roles are required to complete ACF privileged user training. Direct contractor personnel are required to sign a non-disclosure agreement that states that unauthorized disclosures are punishable by pertinent Federal laws.

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

In addition to general security and privacy awareness training, authenticated Content Manager users receive training about using the content management functions. ICF Direct Contractors receive the training courses: Cyber Security Basics, Global Data Protection and ePrivacy. Direct contractors receive Privacy and Cybersecurity training (and Privileged User training, when applicable) from ACF and they sign a Non-Disclosure Agreement (NDA).

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 schedules (retention for a minimum of three years) were agreed upon between the Office of Child Care (OCC) Records Liaison and ACF Records Management Support and have been implemented accordingly. National Archives & Records Retention (NARA) approved disposition authority, see Technical Assistance Records (archives.gov). The schedule number is DAA-0292-2021-0003-0001.

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

Physical security controls are provided by the Acquia platform provider; firewall (technical control) is provided by the direct support contractor; technical controls, such as user identification and password, are provided through the Drupal infrastructure; administrative measures include the privacy training and assuring protection of customer data training that Direct Contractors receive.

Identify the publicly-available URL:

https://childcareta.acf.hhs.gov, https://ecquality.acf.hhs.gov, https://licensingregulations.acf.hhs.gov, and https://pcqc.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.

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