US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

03/10/2022

OPDIV:

ACF

Name:

Peer Technical Assistance

PIA Unique Identifier:

P-6177183-492124

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.

No major changes to the data within Peer Technical Assistance .

Describe the purpose of the system.

The Peer Technical Assistance (PeerTA) application facilitates the sharing of information across state and local agencies implementing the Temporary Assistance for Needy Families (TANF) program. The goal of PeerTA is to establish linkages among TANF agencies and their partners serving TANF and low-income families at the state, county, local, and tribal level. The PeerTA website acts as a dissemination and communications vehicle, supporting the PeerTA Network in the provision of technical assistance, facilitating a dialogue among organizations serving TANF and low-income families, and helping organizations learn about innovative programs and the latest research around effective strategies to successfully support TANF and low-income families on a path to self-sufficiency.

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

The Office of Family Assistance (OFA) PeerTA system collects information to identify individuals representing Federal, State, Local, Tribal organizations who register for an application account. This account provides them with the ability to login to the eLearning System and access courses. The registration aims to help them conveniently access the system (stop/start) course whenever they want.

During the registration process, individuals also self-select a username and password (subject to complexity requirements).

Other types of information included in the system:
Webinar information/transcripts/videos

Toolkits are resources which summarizes and distills the extensive best-practice guidance available in a specific field and then applies this knowledge to the case of TANF

Partners (include Federals, State, and Tribal TANF agencies) websites/resources

The Portable Document Format (PDF) (toolkits, copy of presentations/information delivered during public meetings)
and other resources are available to TANF stakeholders.

TANF stakeholders who have questions or wish to provide feedback provide their email address, name, subject, and question/comment to allow the OFA Team to respond.

PII collected from system administrators/content managers consists of username, password, and email address.

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

The Peer Technical Assistance (PeerTA) application facilitates the sharing of information across state and local agencies implementing the Temporary Assistance for Needy Families (TANF) program. The goal of PeerTA is to establish linkages among TANF agencies and their partners serving TANF and low-income families at the state, county, local, and tribal level. The PeerTA website acts as a dissemination and communications vehicle, supporting the PeerTA Network in the provision of technical assistance, facilitating a dialogue among organizations serving TANF and low-income families, and helping organizations learn about innovative programs and the latest research around effective strategies to successfully support TANF and low-income families on a path to self-sufficiency.

Office of Family Assistance (OFA) PeerTA collects information to identify individuals representing Federal, State, Local, Tribal \ organizations who register for an application account. During the registration process, individuals are required to provide the following information:
E-mail Address
First Name
Last Name
Organization
Organization Type (Federal, State, Local, Tribal, Other)
State
ZIP Code

Optional information that may be provided includes:
City/town

Country

During the registration process, individuals also self-select a username and password (subject to complexity requirements).

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

Yes

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

Organization Type

Organization

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

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

The primary purpose of the PII is to establish system user accounts and respond to questions about the TANF program.

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

Not applicable. There is no secondary use of the PII collected.

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

42 U.S.C. 629e - Title 42-The Public Health And Welfare Chapter 7-Social Security Subchapter Iv-Grants To States For Aid And Services To Needy Families With Children And For Child-Welfare Services Part B-Child and Family Services Subpart 2-promoting safe and stable families.

5 U.S.C. 301 - Title 5-Government Organization and Employees Part I-The Agencies Generally Chapter 3-Powers Subchapter I-General Provisions Jump To: Source Credit Miscellaneous §301.

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

No

Identify the sources of PII in the system.

Identify the OMB information collection approval number and expiration date

OMB Control Number: 0970-0401

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.

Individuals self-register for the PeerTA application and will voluntarily provide their personal information to create a profile within the application. Therefore, no prior notice is given. The PeerTA application also provides a publicly available privacy policy currently available at the following URL: https://peerta.acf.hhs.gov/privacy-policy

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 method in place for the collection of PII as individuals not wishing to provide the information requested have the choice to not register as a system user.

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

All registered users with PeerTA are notified of changes to the application via the banner alert process. In addition, system administers are notified of any disclosures or changes via email.

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 who wish to resolve any issues with their PII can contact peerta@blhtech.com. The ACF Office of Family Assistance (OFA) and the direct contractor will address any issues as they arise.

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

Registered users manage their own account and profile data, and they access the data when they log into their accounts. PII is reviewed annually to confirm validity/accuracy/integrity/availability.

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 approve and validate the Privileged account creation.

The procedures in place to limit access to PII include the following:

Application and system administrators’ access is limited based on the duties they perform within those roles.

Content Managers (communication with end-users) and System Administrators (create content managers account / troubleshoot and support end-users).

End users are self-registered (to access the courses). Registered users only have access to their data. They manage their own account and profile data.

Administrators and Content managers must adhere to ACF policies and procedures and are approved by OFA personnel. Administrators and Content Managers are required to complete ACF Security trainings annually.

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.

System administrators have access to PII (user email address, name, and address) to support and troubleshoot user accounts.

Content Managers have access to PII (email address) to coordinate communication between registered users and to publish technical assistance requests from registered users.

Site controls are segmented by roles: Anonymous, Authenticated user, Content Managers, Administrators.

Permissions limit the needs of each role and protect PII from unauthorized access.

Once roles for accessing the application are assigned/approved by the OFA Account Manager, relevant access is provided.

Roles are managed by System Administrator (upon validation from Account Managers).

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 employees and direct contractors with access to the PeerTA application are subject to HHS ACF security and privacy training and awareness requirements commensurate with the system role in which they function

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

System administrators who manage the virtual systems hosting the PeerTA application must complete Administrators role-based training provided by ACF at the following URL:
Fundamentals of IT Administrators' Roles and Responsibilities (hhs.gov)
https://www.hhs.gov/about/agencies/asa/ocio/cybersecurity/security-awareness-training/index.html

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.

PeerTA is disposed of according to the ACF Archive Schedule: https://www.acf.hhs.gov/digital-toolbox/policy-guidance/acf-archive-schedule.

PII is redacted on the website after an individual enters a question (before publishing). PII is removed when requested by a user and after 1 year of inactivity.

Privileged accounts are reviewed every six months. After the review, Privileged user accounts permissions can be validated, updated, or revoked based on the results of the review and the status of the users.

Disposition actions of electronic records include disposal and destruction of temporary records no longer needed to conduct agency business.

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

Administrative controls: Site Administrators receive regular training in security rules and procedures to protect PII. Training must be completed on an annual basis.
Registered User posts and responses are reviewed for appropriateness prior to being published on the site. Specific user contact information is not published on the site.
Registered users do not have access to the database where PII information is stored. Registered users only have access to their own PII stored in their profile. Role-based access is implemented within the application to enforce access control.

Physical Controls: Employee Data Center Access
AWS provides physical data center access only to approved employees. All employees who need data center access must first apply for access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access and are time-bound. Requests are reviewed and approved by authorized personnel, and access is revoked after the requested time expires. Once granted admittance, individuals are restricted to areas specified in their permissions.
Third-Party Data Center Access
Third-party access is requested by approved AWS employees, who must apply for third-party access and provide a valid business justification. These requests are granted based on the principle of least privilege, where requests must specify to which layer of the data center the individual needs access and are time-bound. These requests are approved by authorized personnel, and access is revoked after request time expires. Once granted admittance, individuals are restricted to areas specified in their permissions. Anyone granted visitor badge access must present identification when arriving on site and are signed in and escorted by authorized staff.
AWS GovCloud Data Center Access
Physical access to data centers in AWS GovCloud (US) is restricted to employees who have been validated as being US citizens.

Technical controls are implemented to limit PII access to that which is associated with the profile of the registered user logging into the application.
Technical Controls: Passwords utilize MD5hashing for encryption.
Database are encrypted using AWS KMS.

Identify the publicly-available URL:

https://peerta.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?

Yes

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

Yes