US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

06/03/2022

OPDIV:

ACF

Name:

Training and Technical Assistance (TTA) Smart Hub

PIA Unique Identifier:

P-6361039-212535

The subject of this PIA is which of the following?

Minor Application (stand-alone)

Identify the Enterprise Performance Lifecycle Phase of the system.

Implementation

Is this a FISMA-Reportable system?

No

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 Training and Technical Assistance (TTA) Smart Hub is a secure, web-based system used for 1) capturing the TTA needs of Head Start grantees, 2) documenting the TTA that grantees receive from Office of Head Start (OHS), and 3) providing data that can be analyzed to assess TTA effectiveness in supporting grantee progress in delivering high-quality services.

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

The system will collect, maintain, and permanently store contractually-required details about TTA provided to the 1,600 OHS grantees who operate 20,000 Head Start classrooms across the country. Report details include: the name and email of the OHS contractor who provided TTA; the IP address of their workstation; the date, duration, location, goal/s and objective/s of the TTA activity; expected follow-up activities; and the name and email of the OHS contractor who approved the report.

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

The system will provide real-time, accessible information on TTA needs, activities and progress

indicators to assure continuous quality improvement. Users with permission enter the TTA Smart Hub system using a single login/Two Factor Authentication (TFA) feature from Head Start Enterprise System, which houses all grantee information. TTA Smart Hub collects the user's IP address.

PII information includes OHS grantee names, work addresses, work phone numbers, work emails, and OHS federal TTA staff names and emails. The source of this PII data is the Head Start Enterprise System (HSES), which houses all grantee information and is covered by its own PIA. TTA Smart Hub and HSES are both OHS information systems. The TTA Smart Hub retrieves grantee information from HSES. (Note: Users also access the TTA Smart Hub via HSES's single login TFA process.)

PII information also includes OHS TTA contractor names, work addresses, work phone numbers, and work emails. The source of this PII is contractor staffing reports that are securely filed by each TTA contract with OHS' Division of Contracts.

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

Yes

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

User credentials

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

OHS-funded Head Start grantees

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

The PII is associated with fulfillment of TTA Activity Reports that are contractually required for OHS TTA contractors.

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

PII will not be used for any secondary purposes.

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.

Identify the OMB information collection approval number and expiration date

Not applicable, as information collected into and/or maintained in the system is not subject to one or more OMB Control Numbers.

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Describe any agreements in place that authorizes the information sharing or disclosure.

An MOU has been executed between the OHS Division of Comprehensive Services and Training and Technical Assistance (owner: TTA Smart Hub) and the OHS Division of Program Operations (owner: HSES).

Describe the procedures for accounting for disclosures.

The MOU executed between the OHS' Division of Comprehensive Services and Training and Technical Assistance and the OHS Division of Program Operations informs the ACF Office of the Chief Information Officer (OCIO) of the data transfer and respective data security plans between TTA Smart Hub and HSES in accordance with the applicable data routine use disclosure.

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

There is currently a Standard Operating Procedure (SOP) in place to account for disclosures.
TTA Smart Hub's System of Record Notice (SORN) describes every routine use of disclosure and to whom it is made. These include data sharing for normal operations based on user roles, restrictions for access based on these roles, and data sharing for third-party analysis. TTA Smart Hub has safeguards in place in the event of an inadvertent sharing or intentional hacking of the system.
There are three types of disclosure that apply to TTA Smart Hub:
1. In the normal operation of TTA Smart Hub, data is shared within the application, using the user roles and organizations to limit who has access to which cases and data sets.
2. In some cases, a dataset is prepared for third party analysis.
3. Inadvertent sharing or intentional hacking of TTA Hub that will cause data to be disclosed.

Is the submission of PII by individuals voluntary or mandatory?

Mandatory

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.

No opt-out is provided because the TTA Smart Hub supports the submission of TTA Activity Reports, which are deliverables for the contracts providing OHS's regional TTA services. The contractually required deliverables are the TTA Activity Reports that document TTA services delivered to OHS grantees.

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

When there are major changes to the system that require notification and consent of individuals, TTA Smart Hub administrators notify the OHS Regional Office Contracting Officer's Representatives (CORs) by email, so they can notify the Regional TTA contract manager. Each TTA contract manager will be responsible for notifying their TTA contract staff, who comprise most of our user base.
OHS Central Office leadership will be notified by email by the OHS Product Owner for awareness.

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 TTA Smart Hub uses PII (as defined above) from the staffing rosters of the 12 Regional TTA Contracts that are directly managed by Regional CORs. Updates for contractor names and contact information are handled through CORs and reported to the OHS Division of Contracts.

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: Data integrity of the PII collected in security artifacts is maintained by restricting edit privileges for all artifacts to those users who have been approved. Privileges are set to control access by user type and by each system. All user account requests to add, remove, or modify must be submitted by account managers to the Government Technical Monitor (GTM) for approval. We conduct periodic reviews of the contractor's staffing roster and match users against the list of permission roles.

Availability: All data, including PII, is reviewed for Availability through our comprehensive test suite and continuous monitoring system. An ACF and Amazon Web Services (AWS) Service Level Agreement states that AWS will provide a monthly up-time percentage of at least 99.9%. Additionally, OCIO Operations will be taking backups of the system data, including the PII every 24 hours, as described in the Business Impact Assessment (BIA).

Data Accuracy: PII is cross-checked against the relevant staffing roster filed with the OHS Division of Contracts before users can gain access to the TTA Smart Hub.

Data Relevancy: The relevancy of the data is maintained by following the specific retention and destruction schedules outlined in the approved OHS Records Management Policy. In addition, user accounts are disabled after 60 days of non-use.

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.

The Product Owner (PO) and System Administrator have mapped the user types and associated permissions to limit exposure of PII.

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 system requires role-based authorization for all users. Only a limited number of System Admins, using Government Furnished Equipment (GFE), have access to PII.

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.

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

The primary users who are trained on the MVP of the TTA Smart Hub are: User 1) ~300 Regional TTA Specialists who enter data into the activity report (AR), and User 2) ~30 Regional TTA Managers who approve the reports.

We previously trained these users in the form content, so the TTA Smart Hub's Minimally Visible Product (MVP) will have familiar data labels, terms, and fields. We are confident that users understand the content because they are currently providing this data in an interim version of the TTA Activity Report (AR) in SmartSheet.gov. More than 3,500 ARs have been submitted since Sept. 15, 2020. The User Guide was created for those trainings and will be adapted.

We train each user group on the presentation of TTA Hub navigation, how to enter and save data, sharing and submitting ARs, and AR approval notification processes. Our users are already familiar with form-based AR data and the submission and approval workflows. The User Guide created for the SmartSheet.gov instance will be updated to reflect completion of the AR in the TTA Hub.

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.

All data is being retained until a final schedule is published. At present, OHS Records and Information Management Specialist has provided an approved OHS Records Policy and email instruction that all records in the OHS Smart Hub shall be retained for six years following the end of the grantee’s contract period.

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

Administrative: PII is only accessible to users if they have been granted permission using RBAC to view it for each individual system. There is also annual security awareness training for all users holding accounts for the system.

Technical: All traffic is between end users and the authorization boundary is sent with HTTPS over port 443. PII is encrypted during transit by TLS 1.2 and at rest using AES-256 full-disk encryption, as managed by cloud.gov and Amazon Web Services. Authentication is be provided using the ACF Multi-Factor Authentication Solution. 60 day password change interval, and a maximum failed login attempt of 3 is enforced by the system. System and application logs are reviewed and analyzed on a monthly basis until the automated auditing system is set up using Splunk.

Physical: Physical compute and storage services are physically secured by Amazon Web Services. The physical controls are all inherited by the AWS platform and include the following: Restricting physical access to the data center both at the perimeter and at building ingress points through the help of video surveillance, intrusion detection systems, and 2 rounds of two-factor authentication for each individual accessing a data center floor. Visitors and contractors are required to have ID, sign-in with building security, and be escorted by an authorized staff at all times. Also in place are the Fire detection and suppression systems, Uninterruptible Power Supply (UPS), Climate and Temperature control, and Preventative maintenance.