US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

07/11/2017

OPDIV:

SAMHSA

Name:

Center for the Application of Prevention Technologies

PIA Unique Identifier:

P-8595220-734543

The subject of this PIA is which of the following?

Minor Application (stand-alone)

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)?

No

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

Describe the purpose of the system.

SAMHSA's Center for the Application of Prevention Technologies (CAPT) is a national training and technical assistance (T/TA) system committed to strengthening prevention systems and building the nation's behavioral health workforce. Administered by the Center for Substance Abuse Prevention (CSAP), the CAPT supports the delivery of effective prevention programs and practices to address these problems. To support these efforts, the CAPT operates several stand-alone technology applications as part of its overall system: CAPT Services Database, CAPT Connect and CAPT Online Training Portal. The CAPT Services Database is the CAPT's primary web-based task order project management and performance monitoring system (as required under the current task order). The CAPT Connect event registration and training and technical assistance (T/TA) resource portal facilitates and manages the delivery of CAPT events and supporting resources to SAMHSA prevention grantee representatives and other relevant audiences. The CAPT Online Training Portal facilitates and manages the delivery of CAPT online courses (both moderated and self-paced) to client representatives and other relevant audiences, as well as the public.

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

SAMHSA's Center for the Application of Prevention Technologies (CAPT) is a national training and technical assistance (T/TA) system committed to strengthening prevention systems and building the nation's behavioral health workforce. The CAPT operates several stand-alone technology applications as part of its overall system:

CAPT Services Database: (a) SAMHSA prevention grantee T/TA needs and service plans to address those needs; (b) service approval forms, with associated labor and travel cost information for individuals managing or delivering the service, supporting materials, field notes for in-person events, and actual costs following event completion; (c) evaluation and follow-up feedback data for specific virtual or in-person T/TA events; (d) evaluation and follow-up feedback data for overall T/TA to address a particular need of a SAMHSA prevention grantee; (e) documentation produced during the annual service planning consultations with SAMHSA prevention grantees regarding the needs, activities, and accomplishments of their epidemiological workgroups; (f) email addresses and passwords, contact information including phone numbers and mailing addresses, organizational affiliation, hourly rate and overhead calculations, administrative documents (e.g., contract scopes of work), and notes on performance and expertise for staff and consultants including photographic identifiers; and (g) contact information and state, tribe, or jurisdiction affiliation for SAMHSA prevention grantee representatives and state project officers.

CAPT Connect: (a) event-specific information, including dates and times, intended audience, presenters with photographic identifiers, and related materials; (b) resource portals supporting specific events or grant recipients; and (c) email addresses and passwords, contact information including phone number, and basic demographic information for individual users (including both system administrators and SAMHSA prevention grantee representatives and other end users including CAPT and SAMHSA staff).

CAPT Online Training Portal: (a) email addresses and passwords for individual users (including both system administrators and SAMHSA prevention grantee representatives and other end users including CAPT and SAMHSA staff); (b) feedback on polls, quizzes, and other interactive learning elements and modules; (c) moderated course forum participation/comments; and (d) course-specific progress and completion data.

All system users are non-direct contractors; no users use HHS credentials to access the system. All non-direct contractors who have access to the system must use individual credentials (a unique user identification and secure password) in order to access each system. The password meets Federal Information Security Management Act (FISMA) requirements for complexity and expiration and the account requires email verification.

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

CAPT Services Database: offers analytic and reporting capabilities to manage field requests, CAPT internal operations, and the delivery of specific services. It streamlines review and approval of planned services, tracks estimated and actual costs to facilitate rapid monitoring of task order spending, manages consultant availability and assignment, and supports ongoing monitoring and evaluation activities. Active users with access to the database are all internal CAPT staff members and contractors (i.e., not consultants, client representatives, state project officers, or other SAMHSA staff or other federal contractors) who enter planned service records, generate tracker forms for Contract Officer Representative (COR) review and approval, submit supporting materials to a quality assurance review process, and enter and generate reports from follow-up evaluation efforts. All data are entered manually by these individual staff members. Reports and analyses generated from the data may be reported to SAMHSA and/or client representatives.

CAPT Connect: streamlines and centralizes processes related to virtual (i.e., online) event registration and participation, developing and sending transactional emails (e.g., confirming registration, issuing reminders and access information, providing follow-up materials and other resources), assembling and transmitting to evaluators event registration and participation lists, and generating certificates of participation (historically, CAPT client representatives completed a new registration form for each event in which they were interested in participating). In addition, the application provides access to relevant T/TA resources. These portals are structured mini-websites of CAPT and other materials related to a particular grant, topic, or audience.

CAPT Online Training Portal: facilitates enrollment and participation in moderated and self-paced CAPT online courses using a course identification number and an enrollment key received from their state, tribe, or jurisdiction. In addition, a select number of self-paced courses are also available to public users. Most courses include certificates of completion and many are facilitated with moderated discussion forums, quizzes, and real-time polls. Course content data is created and/or uploaded manually into the platform.

All system users are non-direct contractors; no users use HHS credentials to access the system. All non-direct contractors who have access to the system must use individual credentials (a unique user identification and secure password) in order to access each system. The password meets Federal Information Security Management Act (FISMA) requirements for complexity and expiration and the account requires email verification.

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

Yes

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

Name

Photographic Identifiers

E-Mail Address

Mailing Address

Phone Numbers

Certificates

Service approval forms, with associated labor and travel cost information for individuals managing or

User credentials are required in order to log into each of the systems. As users attend events, earn certificates and update their contact information, this information needs to be kept safe within their own unique account, thus requiring user credentials, which is a unique user identification and secure password, in order to access each system.

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

Employees

Public Citizens

Business Partner/Contacts (Federal/state/local agencies)

Vendor/Suppliers/Contractors

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

CAPT Services Database: (a) controlling system access; (b) facilitating content approval workflows and notifying appropriate users upon workflow state transitions; (c) maintaining an internal directory of contact information for staff, casual employees, consultants, and subcontractors; (d) ensuring that appropriate individuals are available for service planning, management, and delivery; and (e) contacting SAMHSA prevention grantee representatives for to solicit follow-up evaluation feedback.

CAPT Connect: (a) controlling system access; (b) facilitating content approval workflows and notifying appropriate user upon workflow state transitions; (c) sending appropriate transactional emails to individual users when they register for events or otherwise; (d) registering users for particular events and granting them access to particular portals, (e) generating participant lists for follow-up evaluation and reporting to SAMHSA; and (f) generating certificates of participation for event registrants automatically.

CAPT Online Training Portal: (a) controlling system access; (b) enrolling users in particular self-paced and moderated online courses; (c) monitoring participant progress and course completion status; (d) generating certificates of completion for course participants; and (e) generating course participant lists for follow-up evaluation and reporting to SAMHSA.

None of these Users are direct contractors; no users use HHS credentials to access the system. All non-direct contractors who have access to the system must use credentials (a unique user identification and secure password) in order to access each system and the account requires email verification.

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

Not applicable.

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

Section 501(d)(4) of the Public Health Service Act (42 USC 290aa)—Data Collection.

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

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

Not applicable.

SORN is In Progress

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Hardcopy

Email

Online

Government Sources

Within OpDiv

State/Local/Tribal

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

OMB No. 0930-0197, Exp. Date 1/31/20.

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.

CAPT Services Database: (a) contact information, organizational affiliation, and mailing addresses are entered for CAPT personnel (i.e., staff, casual employees, consultants, and subcontractors) upon hiring or contract execution (i.e., notice prior to collection is not provided); (b) email addresses and state, tribe, or jurisdiction affiliation for SAMHSA prevention grantee representatives and state project officers are entered periodically using contact lists supplied by SAMHSA (i.e., notice prior to collection is thus not applicable); and (c) email addresses for T/TA service recipients is requested at the time of service delivery with individuals given an explanation of why information is being requested and for what purposes it will be used (i.e., formal notice of collection is provided).

CAPT Connect: all PII (email address and password, contact information, and demographic information) is supplied and maintained by individuals when they create an account or access the system in the future, and notification of the purpose, burden, and intended use of the information is provided as part of the user profile form (i.e., formal notice of collection is provided).

CAPT Online Training Portal: all PII (email address and password, contact information, and demographic information) is supplied and maintained by individuals when they create an account or access the system in the future—however, currently no notification of the purpose, burden, and intended use of the information is provided as part of the user account creation form (i.e., notice prior to collection is not provided).

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.
CAPT Services Database: (a) email addresses are required for user authentication, so users may not opt-out of the PII collection described in above because they otherwise could not perform the duties of their job; (b) PII collected for SAMHSA prevention grantee representatives and state project officers is collected from lists provided by SAMHSA (as noted above) and, thus, opt-in/opt-out methods are not applicable; and (c) T/TA service recipients are notified at the time of collection that they may object to the collection or use of PII (can opt-out).

CAPT Connect & CAPT Online Training Portal: email addresses are required for user authentication, so while users may choose to opt-out of the PII collection described above they would be canceling their accounts. In addition to the email address, the account form also requires submission of other contact information, though all demographic information is not required. Information collected through the user account form is the same as that which is collected using existing paper-based registration and participation forms approved as part of the Office of Management and Budget (OMB) umbrella package that covers the CAPT task order.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.
CAPT Services Database: (a) CAPT personnel (i.e., staff, casual employees, consultants, and subcontractors) are notified whenever significant changes are made the CAPT Services Database that might affect their work and how the application's data may be used; (b) as contact information for SAMHSA prevention grantee representatives and state project officers is only stored in order to solicit follow-up evaluation feedback--and, moreover, as this contact information is provided by SAMHSA--no process is in place for notification and collection of informed consent; and (c) collection, storage, and reporting on data supplied by individual recipients of CAPT services (including PII) is guided by strict adherence to the OMB umbrella package under which the CAPT is subsumed—any modifications to which are subsequently reflected in the language used to introduce the use of data collection instruments.

CAPT Connect: collection, storage, and reporting on data supplied by individual recipients of CAPT services (including PII) is guided by strict adherence to the OMB umbrella package under which the CAPT is subsumed—any modifications to which are subsequently reflected in the language used in the user account form and in the introductory content on the front page that describes the purpose of the application and how the user's data is used.

CAPT Online Training Portal: collection, storage, and reporting on data supplied by individual recipients of CAPT services (including PII) is guided by strict adherence to the OMB umbrella package under which the CAPT is subsumed. While no OMB or Personal Authentication Service (PAS) language appears on the user account form, any significant modifications to the way in which PII is used would be reflected in the language describing the application (the "About" and "FAQ" sections).

No process to notify and obtain consent is provided since the use of this program and system is entirely voluntary for the public, and contractors must provide PII in order to obtain system access. System Users/Administrators are informed that to be issued a CAPT account, they need to submit the required information. The SAMHSA warning text is displayed on the login page. When a user registers for an event, there is also an OMB warning on that page.

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.

CAPT Services Database: (a) for CAPT personnel (i.e., staff, casual employees, consultants, and subcontractors), no formal process exists, but system administrators routinely update user information and request that individuals who have PII in the application review that data and correct any inaccuracies related to their email address, organizational affiliation, title, and mailing address; (b) because PII for SAMHSA prevention grantee representatives and state project officers is collected from lists provided by SAMHSA the CAPT does not maintain any formal process itself for learning of and resolving individual concerns regarding that contact information; and (c) the PAS that introduces the feedback forms used at the conclusion of a T/TA event includes instructions for contacting the SAMHSA Reports Clearance Officer regarding any aspect related to the collection of individual data—that office would be, then, responsible for instituting a process for ensuring that any concerns raised are considered, investigated, and resolved.

CAPT Connect: the PAS that is displayed on the user account form includes instructions for contacting the SAMHSA Reports Clearance Officer regarding any aspect related to the collection of individual data. In addition, the application includes a "Terms of Use" as well as references throughout to SAMHSA's Privacy Policy, which details how and what kind of information is collected. However, given that all users maintain their own records (i.e., accounts) in the application, then they can independently amend or correct any PII that they have provided.

CAPT Online Training Portal: the application does not currently provide instructions detailing any defined process for addressing concerns regarding the PII of individual users. However, given that all users maintain their own records (i.e., accounts) in the application, then they can independently amend or correct any PII that they have provided.

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

CAPT Services Database: (a) changes to staff employment details (e.g., rate changes, human resources mailing address updates) trigger an immediate update to the particular individual's record, and every month site administrators review existing user accounts to ensure appropriate levels of access; (b) periodically (approximately every three months) new lists, or updates to existing lists, containing the contact information for SAMHSA prevention grantee representatives and state project officers are translated into updates to the corresponding records in the system; and (c) given that only email addresses are collected and stored for service delivery recipients, the CAPT does not have any process in place for periodic review of that information. To ensure that PII and other user-specific data are not inadvertently/improperly modified/destroyed, only a select number of users can update records for individuals. In addition, scheduled automatic backups of the database are conducted daily and backups of the entire application (i.e., database, files, and code) are made to tape each night (daily backups are kept for 2 weeks, a weekly backup is kept for 6 months, and monthly backups are kept for 3 years).

CAPT Connect: periodically (approximately every three months) existing user accounts are reviewed to ensure appropriate levels of access. In addition, every three months users are required to review their account information—including PII—and update thedata to ensure currency and accuracy. Lastly, backups of the entire application (i.e., database, files, and code) are made to tape each night (daily backups are kept for 2 weeks, a weekly backup is kept for 6 months, and monthly backups are kept for 3 years).

CAPT Online Training Portal: periodically (approximately every three months) existing user accounts are reviewed to ensure appropriate levels of access. In addition, backups of the entire application (i.e., database, files, and code) are made to tape each night (daily backups are kept for 2 weeks, a weekly backup is kept for 6 months, and monthly backups are kept for 3 years).

Identify who will have access to the PII in the system and the reason why they require access.

Users:

CAPT Services Database: (a) access the staff directory; (b) identify appropriate SAMHSA prevention grantee representatives for solicitation of follow-up feedback; and (c) select appropriate individuals (based on title and other details) for service delivery or management. CAPT Connect & CAPT Online Training Portal: no end users have access to others' PII.

Administrators:

CAPT Services Database: (a) update records as needed to ensure currency and accuracy and (b) address any problems with user access. CAPT Connect: (a) update records as needed to ensure currency and accuracy; (b) address any problems with user access; and (c) export registration lists to facilitate evaluation activities related to a particular event. CAPT Online Training Portal: (a) update records as needed to ensure currency and accuracy and (b) address any problems with user access.

.

Developers:
CAPT Services Database, CAPT Connect, & CAPT Online Training Portal: (a) update records as needed; and (b) address any problems with user access.

Contractors:
In addition to Users, Developers, and Administrators (all CAPT staff members), this includes subcontracted CAPT staff located in two regional offices. They are considered internal project staff, they are not external users. CAPT Services Database: (a) update records as needed to ensure currency and accuracy and (b) address any problems with user access. CAPT Connect: (a) update records as needed to ensure currency and accuracy; (b) address any problems with user access; and (c) export registration lists to facilitate evaluation activities related to a particular event. CAPT Online Training Portal: (a) update records as needed to ensure currency and accuracy and (b) address any problems with user access.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.
CAPT Services Database: sensitive data such as a staff member's actual hourly rate is only visible by directors and other higher-level managers who already have access to that information through other internal systems, budgets, or otherwise. However, all "users" in this application are internal staff members, who, once authenticated, have access to PII for CAPT personnel. Note, too, that many of the types of individuals described above overlap. A small core group of administrators manages the permissions granted to individual users.

CAPT Connect: administrators responsible for overall site maintenance, as well as those who are responsible for the creation and management of particular T/TA events, can access the registration lists for such events—all such users are CAPT staff members who either coordinate delivery of, or conduct evaluation activities for, T/TA events. Note, too, that many of the types of individuals described above overlap. A small core group of administrators manages the permissions granted to individual users.

CAPT Online Training Portal: only a select few administrators and developers have access to participant information and account information for other users. Note, too, that many of the types of individuals described above overlap.

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.
CAPT Services Database & CAPT Connect: access to the data in these two applications is controlled by a system of fine-grained permissions that are organized by "roles", which are assigned to individual users who share similar functions (e.g., operate in a similar place along a particular content approval workflow), and "groups" (e.g., operate on the same team). These controls allow administrators the ability to grant or revoke access to the data field-by-field .

CAPT Online Training Portal: as noted in above, only a select few administrators and developers have access to participant information and account information for other users. They have full back-end administrative access, allowing them to see complete user account records (including participation logs).

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 Education Development Center, Inc. (EDC; contractor responsible for implementation of the CAPT task order) employees are required to partake in annual security awareness training. New employees are given a standard grouping of modules to ensure a baseline understanding. In subsequent years, employees are given a subset of new hire modules, plus a rotating set of more specialized, but still pertinent, modules to enhance understanding. For those employees in roles of heightened risk, or who require specific compliance-based training, additional role-based modules (e.g. PCI-DSS) are assigned. Lastly, certain non-work related modules are made available as optional material. All available modules are reviewed by EDC annually, and course agendas are updated as needed. EDC makes use of SANS's Securing the Human (http://www.securingthehuman.org/enduser) learning system for its security awareness training program. SANS is a well-respected security organization, and its end user training is founded on the SANS 20 Critical Security Controls in combination with an advisory board of SANS top instructors and industry leading experts.

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

Not applicable.

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.

Per HHS General Technology Management Records,
data is retained for the life of the contract plus 5 years. The general records schedule is currently in internal review and will be updated once the approval comes from the National Archives and Records Administration.

B311, Item 8; Program Evaluation Files: These files consist of historical record or reported or published results, along with pertinent background material of program evaluation studies funded under 1% legislative authority. The official file consists of the Project Description and Justification, approval documents, final reports and implementation documents.

Permanent Disposition: Retain official program evaluation files in respective areas. After receipt of final report put in inactive files and hold for 5 years. Retire to FRC and offer to the National Archives when 10 years old. Background material and other non-official items may be destroyed when no longer needed for reference purposes.

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

Physical controls will be managed at Acquia, an approved Cloud Service Provider (CSP) under the Federal Risk and Authorization Program (FedRAMP). Multiple technical controls are in place, including minimum password requirements to ensure only appropriate users have access to the system, role-based access to ensure authorized users are granted access to data and activities commensurate with their work, and multi-factor requirements for those with elevated access to back-end views or actions to protect against unauthorized code-level changes. Administratively, policies and procedures provide appropriate oversight, including Account Management, Change Management, and Vulnerability Management.

Identify the publicly-available URL:

CAPT Services Database   https://captservices.edc.org
CAPT Connect - https://captconnect.edc.org
CAPT Online Training Portal - https://captonline.edc.org
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.

Session Cookies that do not collect PII.

Other technologies that do not collect PII:

Google Analytics

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?

No