Save

Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-18476 | Form Date: 4/12/2019 9:53:36 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-3926416-504486
2a	Name:	CBA Tracking System (CTS)
3	The subject of this PIA is which of the following?	○ General Support System (GSS) ○ Major Application ○ Minor Application (stand-alone) ◉ Minor Application (child) ○ Electronic Information Collection ○ Unknown
3a	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
3b	Is this a FISMA-Reportable system?	○ Yes ◉ No
4	Does the system include a Website or online application available to and for the use of the general public?	○ Yes ◉ No
5	Identify the operator.	◉ Agency ○ Contractor
6	Point of Contact (POC):	POC Title: IT Security Steward POC Name: Carman Layne POC Organization: NCHHSTP/DDID POC Email: iws6@cdc.gov POC Phone: 770.488.8116
7	Is this a new or existing system?	◉ New ○ Existing
8	Does the system have Security Authorization (SA)?	○ Yes ◉ No
8b	Planned Date of Security Authorization	July 12, 2019 ☐ Not Applicable

Save

11	Describe the purpose of the system.	CBA Tracking System (CTS) is a secure browser-based (Internet) application allowing CDC and its public partners to cooperate in the delivery of HIV/AIDS prevention services. The application allows CDC-Funded Community-Based Organizations (CBOs) and State and Local Health Departments (SHDs/LHDs) to request Capacity Building Assistance (CBA) services and enable CDC to match these requests with CBA providers. CTS also allows providers to report on the status of capacity building activities, request additional services from other CBA providers, and provide visibility of activities to all participants.
12	Describe the type of information the system will collect, maintain (store), or share. (Subsequent questions will identify if this information is PII and ask about the specific data elements.)	The CTS system is a secure browser-based (Internet) application allowing CDC and its public partners to cooperate in the delivery of HIV/AIDS prevention services. CBA coordinators are required to register and enter user ID and passwords to enter CBA requests in CTS via a wizard that walks the requester through the process step by step. The CTS coordinator tells the system to send an e-mail to the selected CBA provider to confirm the request assignment. No personally identifiable information (PII) is sent to CTS for validation. A separate CTS Administration (CTS Admin) module provides access for authorized CBA providers to control certain aspects of the reporting processes within both CTS and CBAE. Users and Organization data is collected and stored temporarily to include: name, business email, business phone number, organization name, type, funding type and business address. This information is required for management-level reporting. Data elements can be selected in CTS Admin for reporting which includes: request status, regions, health dept types, race for requests, risk for requests, special population for requests, gender for requests, HIV status, venue types, needs contact types, contact types, CBA Reports Management System (CRMS) status, strategic plan/assessment status and HIV Status demographics. No personally identifiable information (PII) is sent to CTS Admin for validation.

Save

13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The CBA Tracking System (CTS) allows CDC-Funded Community-Based Organizations (CBOs) and State and Local Health Departments (SHDs/LHDs) to request Capacity Building Assistance (CBA) services and enable CDC to match these requests with CBA providers. CTS also allows providers to report on the status of capacity building activities, request additional services from other CBA providers, and provide visibility of activities to all participants. CBA requests are entered in CTS. Once submitted, the CBA Coordinator, Program Consultant, and project officer manage the requests through the CTS Admin module which is accessible via the CDC intra net only. The CBA Coordinator tells the system to send an e-mail to the selected CBA provider to confirm the requested assignment. The CBA provider then enters contact times, plans for fulfilling the request, and other information. The system also provides analytical and transactional reporting. No personaly identifiable information (PII) is sent to CTS for validation. The CTS Administration (CTS Admin) module collects the Organization's business address, State and Zip Code only, and the business email address of the individual requesting to retrieve reports. CBA providers can also select data elements for reporting which includes: request status, regions, health dept types, race for requests, risk for requests, special population for requests, gender for requests, HIV status, venue types, needs contact types, contact types, CBA Reports Management System (CRMS) status, strategic plan/assessment status and HIV Status demographics. No personally identifiable information (PII) is sent to CTS Admin for validation.
14	Does the system collect, maintain, use or share **PII**?	(•) Yes ( ) No

Save

15	Indicate the type of PII that the system will collect or maintain.	☐ Social Security Number ☐ Date of Birth ☐ Name ☐ Photographic Identifiers ☐ Driver's License Number ☐ Biometric Identifiers ☐ Mother's Maiden Name ☐ Vehicle Identifiers ☒ E-Mail Address ☒ Mailing Address ☒ Phone Numbers ☐ Medical Records Number ☐ Medical Notes ☐ Financial Account Info ☐ Certificates ☐ Legal Documents ☐ Education Records ☐ Device Identifiers ☐ Military Status ☐ Employment Status ☐ Foreign Activities ☐ Passport Number ☐ Taxpayer ID Organization's business State and Zip Code User IDs and passwords
16	Indicate the categories of individuals about whom PII is collected, maintained or shared.	☒ Employees ☐ Public Citizens ☒ Business Partners/Contacts (Federal, state, local agencies) ☐ Vendors/Suppliers/Contractors ☐ Patients Other
17	How many individuals' PII is in the system?	500-4,999
18	For what primary purpose is the PII used?	Information is subsequently used for management-level reporting and to email individuals their course completion certificates.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	N/A
20	Describe the function of the SSN.	N/A
20a	Cite the **legal authority** to use the SSN.	N/A
21	Identify **legal authorities** governing information use and disclosure specific to the system and program.	Public Health Service Act, Section 301, "Research and Investigation," (42 U.S.C. 241); and Sections 304, 306 and 308(d) which discuss authority to maintain data and provide assurances of confidentiality for health research and related activities (42 U.S.C. 242 b, k, and m(d)).
22	Are records on the system retrieved by one or more PII data elements?	○ Yes ◉ No

Save

23	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains ☒ In-Person ☐ Hard Copy: Mail/Fax ☒ Email ☐ Online ☐ Other Government Sources ☐ Within the OPDIV ☐ Other HHS OPDIV ☐ State/Local/Tribal ☐ Foreign ☐ Other Federal Entities ☐ Other Non-Government Sources ☐ Members of the Public ☐ Commercial Data Broker ☐ Public Media/Internet ☒ Private Sector ☐ Other
23a	Identify the OMB information collection approval number and expiration date.	0906-0022, 01/31/2020
24	Is the PII shared with other organizations?	○ Yes ◉ No
25	Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.	Yes users are notified by other means. A warning banner notifies CTS end users at login that by using this system, you understand and consent to the following: The Government may monitor, record, and audit your system usage, including usage of personal devices and email systems for official duties or to conduct HHS business. Therefore, you have no reasonable expectation of privacy regarding any communication or data transiting or stored on this 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 system. Any communication or data transiting or stored on this system may be disclosed or used for any lawful Government purpose.
26	Is the submission of PII by individuals voluntary or mandatory?	◉ Voluntary ○ Mandatory
27	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.	User name, business phone, address and business email are required to establish access to the CTS Admin module and for management-level reporting. If the individual does not want to provide his or her business information, he or she may not access the system.

Save

28	Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection). Alternatively, describe why they cannot be notified or have their consent obtained.	E-mail notifications are sent to CTS users (requesters, recipients, CBA providers, and CDC staff) to notify them about the status of or changes to a CBA request.
29	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. If no process exists, explain why not.	CTS CBA resources are available 24-hours per day 7 days a week. Users can submit a new request, check the status of a previous request, and perform many other system functions any time.
30	Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. If no processes are in place, explain why not.	PII is reviewed at the time of its use for integrity, availability, and accuracy. Relevancy is reviewed by conducting reviews of systems containing PII, as a part of the Annual Assessment and POAM process or as significant changes occur.
31	Identify who will have access to the PII in the system and the reason why they require access.	☐ Users ☒ Administrators: To maintain and update CTS usability. ☐ Developers ☐ Contractors ☐ Others
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The CTS Business Steward determines who has access to PII data based on their position (i.e. Role-Based Access Controls and Least Privilege) description or contract responsibilities.
33	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.	Least privilege model is utilized based on User ID in conjunction with Active Directory to limit access to files containing PII within the system.
34	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.	Annual CDC Security AwarenessTraining/Role Based Training
35	Describe training system users receive (above and beyond general security and privacy awareness training).	Not Applicable - Any training above and beyond annual CDC required training is optional.
36	Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?	◉ Yes ○ No

Save

37	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.	CTS system does not collect or retain PII. For CTS Admin module, name, business address and phone, and the business email address are retained as long as access to reports are required. This information is used to validate their identity when logging into the CTS Admin module and to enter CBA request into CTS. Records are retained according to the General Records Schedule, GRS-20-01a, Electronic files or records created solely to test system performance, as well as hard copy printouts and related documentation for the electronic files/records. Records are destroyed when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes.
38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Technical controls: CTS administrators data is secured through Windows Active-Directory requiring smart-card login with dual authentication to access. CBA providers come into the application via a secure web site that controls what functions they are allowed perform based upon a "Business Steward" role as assigned by a federal system administrator. Access requires entry of a user identification and system generated password issued directly to only the provider. The data is maintained in a dedicated database with restricted access. Administrative controls: Access is restricted to a limited number of users and is governed by CDC Privacy and Confidentiality policies and the Confidential Information Protection and guidelines. The CTS Administrator(s) roll has access to only their job role/function. Individuals who do not provide contact data will not receive access to the CTS system. Their data is collected for CBA requests and management-level reports. Physical controls: The data center is protected with physical access controls, software and hardware firewalls, and user access authentication.
General Comments		
OPDIV Senior Official for Privacy Signature	Jarell Oshodi -S Digitally signed by Jarell Oshodi -S Date: 2019.05.15 10:43:26 -04'00'	