Save

Privacy Impact Assessment Form

v 1.47.4

Status: Draft   Form Number: F-36958   Form Date: 8/21/2018 8:52:42 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-6816363-513315
2a	Name:	National Youth Tobacco Survey (NYTS)
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.	Development
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: ISSO POC Name: Cindy Allen POC Organization: NCCDPHP POC Email: CDL1@CDC.GOV POC Phone: 770-488-5388
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	December 31, 2018 □ Not Applicable

Save

11	Describe the purpose of the system.	The National Youth Tobacco Survey (NYTS) system is an electronic survey system that collects and stores anonymous
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 system collects and maintains rudimentary responses of survey questionnaires from approximately 20,000 anonymous middle school and high school students annually. The survey is voluntary and students are asked about their behaviors,
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	National Youth Tobacco Survey system is a survey data collection that utilizes mobile Android application tablet devices and a web-based as a front-end client. Survey
14	Does the system collect, maintain, use or share **PII**?	● Yes ○ No
15	Indicate the type of PII that the system will collect or maintain.	☐ Social Security Number ☒ Name ☐ Driver's License Number ☐ Mother's Maiden Name ☒ E-Mail Address ☐ Phone Numbers ☐ Medical Notes ☐ Certificates ☐ Education Records ☐ Military Status ☐ Foreign Activities ☐ Taxpayer ID ☐ Date of Birth ☐ Photographic Identifiers ☐ Biometric Identifiers ☐ Vehicle Identifiers ☐ Mailing Address ☐ Medical Records Number ☐ Financial Account Info ☐ Legal Documents ☐ Device Identifiers ☐ Employment Status ☐ Passport Number User ID Password
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?	The emails will be used to establish an access account in order to allow them to securely accessing the system for administration, development, and maintenance purposes.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	PII is used for communication purposes.

Save

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).
22	Are records on the system retrieved by one or more PII data elements?	○ Yes ● No
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.	N/A
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.	Users are made aware of their PII being collected at the time they are identified as needing access to use the system. PII is collected from the system administrators only, not for the study.
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.	No option for administrators to opt-out of having their user credentials and emails used because it is required for their role. This information is necessary to establish an account in supporting the study and accessing 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.	PII identified is an authentication credential for system administrator. There is no process in place to notify and obtain consent from the individuals when there are major changes occur to the system because those changes would require themselves as an administrator, to perform or take action.	
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.	System administrators may send an email to their supervisor if issues arise. PII is not collected from the study participants so no process is necessary.	
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 identified is an authentication credential for system administrator. There is no process in place to periodically reviews of PII.	
31	Identify who will have access to the PII in the system and the reason why they require access.	□ Users	
		☒ Administrators	System administrator have access to the structures and hardware supporting the information system.
		□ Developers	
		□ Contractors	
		□ Others	
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Administrator is granted access based on their roles as authorized by the project manager and the information system manager. Granulated rights at both application and server	
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.	Role based access controls are in place to ensure the concept of "least privilege" is implemented. Based on the technical director and project director’s assessment of each team member, the network administrator creates and implements network access groups. The access groups include system administrator, data analyst, database administrator, and web developer working on data validation, processing, etc . Each individual assigned to work on the project is assigned to a group associated with their role. Access rights are then derived from that role. The project network directory structure is organized such that access to each sub folder is restricted to one or more network access groups, effectively ensuring that an individual’s access to data containing PII is restricted only to network areas pertaining to tasks the individual is required to perform.	
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.	CDC contractors are required to complete the Information Security Awareness Training (SAT) annually which covers all aspects of systems and data security and confidentiality. Systems and network staff with higher roles and responsibilities are require to complete additional training on contingency plan and disaster recovery training on an annual basis.	

Save

35	Describe training system users receive (above and beyond general security and privacy awareness training).	Systems and network infrastructure staff receive specific security training based on the technology they support on an ongoing basis and receive additional security training as necessary to meet contract requirements.
36	Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?	● Yes ○ No
37	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.	User accounts and associated PII are removed when no longer needed for access. The PII and user accounts are temporary administrative records and not subject to long term records retention. CDC Records Control Schedule GRS-24-13a PKI Administrative Records. User accounts are reviewed annually.
38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	PII identified is an authentication credential for system administrator. Administrative Controls: include a security plan, file back-up, least privilege, and training. Technical Controls: Only the system administrator will have access to the authentication credential. The users' credential will be encrypted at the database level. Physical Controls: include ID Badges, Key Cards, and Closed Circuit TV (CCTV) for servers.

General Comments	
OPDIV Senior Official for Privacy Signature	Jarell Oshodi -S Digitally signed by Jarell Oshodi -S Date: 2018.12.31 15:15:35 -05'00'