Save

Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-49931 | Form Date: 10/24/2017 7:00:24 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-9720560-582766
2a	Name:	National Prevention Information Network (NPIN)
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 Specialist POC Name: William Dolan POC Organization: NCHHSTP/OD POC Email: wdolan@cdc.gov POC Phone: 404.639.6233
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 31, 2019 ☐ Not Applicable

Save

11	Describe the purpose of the system.	The CDC National Prevention Information Network (NPIN) provides the Centers for Disease Control and Prevention a forum for the dissemination of information, and transfer of knowledge, concerning the research, treatment, care, and prevention of human immunodeficiency virus (HIV), Viral Hepatitis, STD, and TB-related disease (TB Education and Training). Consumers include CDC constituents, partners, and the general public. Originally conceived as the CDC National AIDS Clearinghouse designed to facilitate the sharing of information and resources among people working in HIV prevention, treatment, and support services, NPIN has expanded to include other services to become a comprehensive source of science-based information accessible to professionals dedicated to the prevention of HIV, Viral Hepatitis, STDs, and TB . NPIN has been dubbed as the next-generation clearinghouse model for collecting and disseminating data and materials in support of prevention activities within international, domestic, state, and local settings. These services are designed to facilitate program collaboration, sharing information, resources, published materials, research, and trends among the four diseases.
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.)	NPIN is a public website and the information collected includes domain name IP address from which you access the Internet, the date and time you access our site; the pages you viewed; the type of browser and operating system you used to access our site; and, if you linked to our site from another Website, that Web-site's address and email address. When inquiries are sent to NPIN via e-mail, we temporarily store the question(s) and the e-mail address information so that we can respond electronically.
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	NPIN is a public website and the information collected includes: domain name, IP address from which you access the Internet, the date and time you access our site; the pages you
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
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?	100,000-999,999
18	For what primary purpose is the PII used?	The primary purpose of the PII is to notify users of NPIN site updates.
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
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.	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.	Individuals may elect to sign up for website updates, in which case they are asked for their email address to allow the system to send the updates to them.
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.	Individuals who do not want to give their email address can choose not to sign up for the website updates. Opt-out information is provided in the privacy policy.
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.	Any changes impacting disclosure or data use would be updated in the site privacy policy: "Why is information collected?" Individuals would receive notification of updates via email and could then elect to opt out if they choose.
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.	Individuals seeking to contest the content of information about them in this system should contact the system manager via email at NPIN-info@cdc.gov

Save

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.	The email addresses are not held by CDC so there is no review process available. The email address are only held by the IQ Solutions Communications Cloud. As part of our continuous monitoring plan, IQ Solutions conducts a review within every three hundred sixty-five (365) days of PII holdings (i.e. email addresses) to ensure the data's integrity, availability, accuracy and relevancy. For administrative accounts, individual PII (email, name, and telephone number) is only modified by the individual who owns the PII and therefore cannot be inadvertently modified or destroyed by the system. Activities within the system are logged, so any changes to PII can be traced back to a specific time, and user providing non-repudiation within the system. The system is highly available, ensuring the PII is available when needed. The IQ Solutions Communications Cloud is located in a pair of Tier-III datacenters to provide great availability. Hosting the IQ Solutions Communications Cloud in two physically separate datacenters provide an avenue to ensure continuity of service to the public in a case of unforeseen event. The system automatically detects rejected email addresses, and removes those email addresses and all associated records from the system, ensuring that PII is accurate and up to date within the system.
31	Identify who will have access to the PII in the system and the reason why they require access.	☐ Users ☒ Administrators: IQ Solutions have access in order to maintain and test the system. ☐ Developers ☐ Contractors ☐ Others
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	NPIN uses role-based access controls to ensure that administrators, and users are granted access on a 'least privilege' basis commensurate with their assigned duties (only
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.	The least privilege model is utilized to allow those with access to PII to only access the minimum amount of information necessary
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.	IQ Solutions staff with access to the email database attend a Security and Privacy Awareness Training yearly
35	Describe training system users receive (above and beyond general security and privacy awareness training).	None.

Save

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.	The email addresses are active as long as the user opts to receive the updates. The user can opt out by following the Opt-out information provided in the privacy policy found at https://npin.cdc.gov/pages/policies-and-disclaimers#privacy GRS RECORDS SCHEDULE 16 - 02a(01) - Records Disposition Files. Descriptive inventories, disposal authorizations, schedules, and reports. For retention, all PII data is currently kept indefinitely. Granicus does delete any data when an account is shutdown. Granicus will delete all the of Customer Administrators, but there is some history that is retained showing the admin to send a bulletin, or change settings, even after the profiles are deleted. Subscriber information is retained. Typically, although disabled, the return of data is not provided or deleted if a contract is not renewed.

Save

38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Administrative Control: Designated government contracting official or authorized representative designate approves System Administrators. A request to add an Administrator is submitted in writing to the government contracting official or authorized representative and accounts are established in accordance with the access level required based on their role in the organization. It is left to the discretion of the designated CDC contracting official or authorized representative to determine the level of access an Administrator is granted. Physical Control: The IQ Solutions Communications Cloud is built using industry best practices and independently reviewed against Federal Information Security Management Act (FISMA) and National Institute of Science and Technology (NIST) Security and Privacy controls to ensure technical, operational, and management controls are properly applied. Specifically, the systems are located in Tier III data centers with physical security compliant to a FedRAMP moderate baseline based on NIST 800-53 Rev 4. Physical access to datacenters is controlled through management, physical and administrative controls, in turn providing a multilayered, defense-in-depth security infrastructure. The datacenters are physically secured with all exterior doors being locked and badges required for accessing the buildings. There are closed circuit cameras monitoring both the exterior and interior of the building. There are also security guards on duty during all hours of operation. On-site security personnel patrol the interior and exterior of the datacenters 24/7/365. Physical datacenter access requires the use of multifactor authentication mechanisms using a proximity card and a managed biometric system (hand geometry reader or iris scan – depending on data center). Access is also controlled through an approval process, reviewed by both the entity requesting access and datacenter security personnel. Technical Control: Access is logged and access approvals are audited on a monthly basis by the IQ Solutions ISSO. The confidentiality and integrity of passwords used to access the system are protected per salted password hashing. Sensitive portions of the data base are stored in encrypted table spaces.
39	Identify the publicly-available URL:	https://npin.cdc.gov
40	Does the website have a posted privacy notice?	(•) Yes ( ) No
40a	Is the privacy policy available in a machine-readable format?	(•) Yes ( ) No
41	Does the website use web measurement and customization technology?	(•) Yes ( ) No

Save

		Technologies	Collects PII?
41a	Select the type of website measurement and customization technologies is in use and if it is used to collect PII. (Select all that apply)	☐ Web beacons	○ Yes ○ No
		☐ Web bugs	○ Yes ○ No
		☒ Session Cookies	○ Yes ◉ No
		☒ Persistent Cookies	○ Yes ◉ No
		Other...	○ Yes ○ No
42	Does the website have any information or pages directed at children under the age of thirteen?		○ Yes ◉ No
43	Does the website contain links to non- federal government websites external to HHS?		◉ Yes ○ No
43a	Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?		◉ Yes ○ No

General Comments	
OPDIV Senior Official for Privacy Signature	Jarell Oshodi -S Digitally signed by Jarell Oshodi -S Date: 2019.07.22 14:24:15 -04'00'