Save

Privacy Impact Assessment Form

v 1.45

Status Draft | Form Number F-45991 | Form Date 7/1/2014 8:24:38 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-3857651-701959
2a	Name:	World Trade Center Health Program (WTCHP)
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.	Implementation
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: AD Informatics, NIOSH POC Name: Ken McKneely POC Organization: NIOSH POC Email: kxm2@cdc.gov POC Phone: (404) 498-2513
7	Is this a new or existing system?	◉ New ○ Existing
8	Does the system have Security Authorization (SA)?	◉ Yes ○ No
8a	Date of Security Authorization	Oct 3, 2013

Save

11	Describe the purpose of the system.	The purpose of the World Trade Center Health Program system is to protect World Trade Center Health Program information for the medical coverage to the survivors of the September 11th tragedy and their beneficiaries as a result of the James Zadroga 9/11 Health and Compensation Act of 2010.
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.)	Health Care Administration, General Science and Innovations, Personal Identity and Authentication
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	WTCHP obtains PII voluntarily for billing, processing payments, tracking applicant status, research studies and eligibility determinations. WTC Health Program Records are obtained from individual applicants and enrollees, from medical providers who have treated eligible individuals, and from data centers that are repositories of demographic and clinical information about WTC responders and survivors. The system stores information on encrypted file servers.
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 ☒ 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?	50,000-99,999
18	For what primary purpose is the PII used?	PII is obtained voluntarily for billing, processing payments, tracking applicant status, and eligibility determinations.

Save

19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	General Science and Innovations
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); Occupational Safety and Health Act, Section 20, "Research and Related Activities" (29 U.S.C. 669); and the Public Health Service Act, Title XXXIII, "World Trade Center Health Program" (42 U.S.C. §§ 300mm – 300mm-61).
22	Are records on the system retrieved by one or more PII data elements?	○ Yes ◉ No
22a	Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or identify if a SORN is being developed.	Published: Published: Published: ☐ In Progress
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.	0920-0891, expires 12/31/2014
24	Is the PII shared with other organizations?	○ Yes ◉ No

Save

24a	Identify with whom the PII is shared or disclosed and for what purpose.	☐ Within HHS ☐ Other Federal Agency/Agencies ☐ State or Local Agency/Agencies ☐ Private Sector
24b	Describe any agreements in place that authorizes the information sharing or disclosure (e.g. Computer Matching Agreement, Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)).	
24c	Describe the procedures for accounting for disclosures	
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.	Program applicants receive a copy of the WTCHP Privacy Notice found here: http://www.cdc.gov/wtc/pdfs/NPP%20_%20Full%20Page_%20WTC%20Health%20Program.pdf. In addition program applications include the Privacy Act Statement.
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.	The potential claimants will fill out a voluntary eligibility worksheet at their local providers office voluntarily and can opt-out of the collection of PII with the Provider.
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.	If the WTC Health Program makes any changes to disclosures and/or data uses, a revised Notice of Privacy Practices will be made electronically available on the WTC Health Program website and it will be mailed to members WTC Health Program's next annual mailing. Individuals can also request to receive a copy of the current notice as described in the NOTICE OF PRIVACY PRACTICES FOR THE WORLD TRADE CENTER HEALTH PROGRAM http://www.cdc.gov/wtc/pdfs/NPP%20_%20Full%20Page_%20WTC%20Health%20Program.pdf
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.	The Privacy Notice received by the applicant advises them that if he/she believes that his/her privacy rights have been violated, they may file a complaint with the WTC Health Program by calling 1-888-982-4748, or by sending a letter to P.O. Box 7000 Rensselaer, NY 12144 ATTN: WTC Health Program, HIPAA Complaint. They are further advised that theymay also file a complaint with the Department of Health and Human Services Office for Civil Rights by sending a letter to 200 Independence Avenue, S.W., Washington, D.C. 20201, calling 1-877-696-6775, or visiting www.hhs.gov/ocr/privacy/hipaa/complaints/. TTY users should call 1-800-537-7697.

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 System Administrator will continuously monitor the replication of files and file server data for integrity, availability, and accuracy.	
31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users	To protect World Trade Center Health Program information for the medical coverage to the survivors of the September 11th tragedy and their beneficiaries as a result of the James Zadroga 9/11 Health and Compensation Act of 2010.
		☒ Administrators	Troubleshooting and system updates.
		☐ Developers	
		☐ Contractors	
		☐ Others	
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The system owner determines access to the system	
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 and RBAC to limit access to PII.	
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.	All personnel with access to the system complete CDC Annual Security and Privacy Awareness Training.	
35	Describe training system users receive (above and beyond general security and privacy awareness training).	System users and administrators receive CDC Rules of Behavior training in addition to Security Awareness Training.	
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.	Records are retained and disposed in accordance with CDC Electronic Records Control Schedule for NIOSH records. Research records are maintained in the agency for three years after close of the study. WTC Health Program records are transferred to Federal Records Center 15 years after the case file becomes inactive and are destroyed after 75 years. Paper files that have been scanned to create electronic copies are disposed of after the copies are verified. Disposal methods include erasing computer tapes and burning or shredding paper material.	

Save

38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Administrative controls: A database software security package is utilized to control unauthorized access to the system. Access is granted to only a limited number of physicians, scientists, and designated support staff, as authorized by the system manager, to accomplish the stated purposes for which the data in this system has been collected. Physical controls: Hard copy records are kept in locked cabinets in locked rooms. Guard services in the buildings provides screening of visitors and personnel. The limited access, secured computer room contains fire extinguishers and an overhead sprinkler system. Computer workstations and automated records are located in secured areas. Electronic anti-intrusion devices are in operation at the Federal Records Center. Technical controls: Data sets are password protected and/or encrypted. Protection for computerized records both on the mainframe and the NIOSH Local Area Network (LAN) includes programmed verification of valid user identification code and password prior to logging onto the system, mandatory password changes, limited-login attempts, virus protection, and user rights/file attribute restrictions. Password protections imposes user name and password login requirements to prevent unauthorized access. Each user name is assigned limited access rights to files and directories at varying levels to control file sharing. There are routine daily backup procedures and secure off-site storage is available for backup tapes.

REVIEWER QUESTIONS: The following section contains Reviewer Questions which are not to be filled out unless the user is an OPDIV Senior Officer for Privacy.

	Reviewer Questions	Answer
1	Are the questions on the PIA answered correctly, accurately, and completely?	◯ Yes ◯ No
Reviewer Notes		
2	Does the PIA appropriately communicate the purpose of PII in the system and is the purpose justified by appropriate legal authorities?	◯ Yes ◯ No
Reviewer Notes		
3	Do system owners demonstrate appropriate understanding of the impact of the PII in the system and provide sufficient oversight to employees and contractors?	◯ Yes ◯ No
Reviewer Notes		
4	Does the PIA appropriately describe the PII quality and integrity of the data?	◯ Yes ◯ No
Reviewer Notes		

Save

	Reviewer Questions	Answer
5	Is this a candidate for PII minimization?	◯ Yes ◯ No
Reviewer Notes		
6	Does the PIA accurately identify data retention procedures and records retention schedules?	◯ Yes ◯ No
Reviewer Notes		
7	Are the individuals whose PII is in the system provided appropriate participation?	◯ Yes ◯ No
Reviewer Notes		
8	Does the PIA raise any concerns about the security of the PII?	◯ Yes ◯ No
Reviewer Notes		
9	Is applicability of the Privacy Act captured correctly and is a SORN published or does it need to be?	◯ Yes ◯ No
Reviewer Notes		
10	Is the PII appropriately limited for use internally and with third parties?	◯ Yes ◯ No
Reviewer Notes		
11	Does the PIA demonstrate compliance with all Web privacy requirements?	◯ Yes ◯ No
Reviewer Notes		
12	Were any changes made to the system because of the completion of this PIA?	◯ Yes ◯ No
Reviewer Notes		

General Comments	

OPDIV Senior Official for Privacy Signature	Beverly E. Walker -S Digitally signed by Beverly E. Walker -S DN: c=US, o=U.S. Government, ou=HHS, ou=CDC, ou=People, 0.9.2342.19200300.100.1.1=1001440343, cn=Beverly E. Walker -S Date: 2014.08.11 18:21:37 -04'00'	HHS Senior Agency Official for Privacy	