Save

Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-50666 | Form Date: 3/22/2017 8:58:16 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-6899561-396120
2a	Name:	National Program of Cancer Registries/Cancer Surveillance System (NPCR-CSS)
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: NCCDPHP ISSO POC Name: Cindy Allen POC Organization: NCCDPHP POC Email: clallen@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	August 31, 2018 ☐ Not Applicable

Save

9	Indicate the following reason(s) for updating this PIA. Choose from the following options.	☒ PIA Validation (PIA Refresh/Annual Review) ☐ Anonymous to Non-Anonymous ☐ New Public Access ☐ Internal Flow or Collection ☐ Commercial Sources ☐ Significant System Management Change ☐ Alteration in Character of Data ☐ New Interagency Uses ☐ Conversion
10	Describe in further detail any changes to the system that have occurred since the last PIA.	
11	Describe the purpose of the system.	The National Program of Cancer Registries Cancer Surveillance System (NPCR-CSS) collects, records, and analyzes patient cancer data and generates statistical outputs and reports on cancer incidence in 46 states, the District of Columbia, Puerto Rico, Virgin Islands, and U.S. Pacific Island jurisdictions. NPCR-CSS also aggregates and disseminates cancer incidence data.
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.)	NPCR-CSS collects, aggregates and shares cancer incidence data including: -cancer patient histology and behavior -patient date of birth -state/county of residence -date of diagnosis -race/ethnicity -age at diagnosis -gender -stage at diagnosis -first course of treatment -postal code of residence -Census Tract of residence Also, the system collects users' names, email addresses, and telephone numbers in order to set up the user accounts. CDC employees do not access the system. Cancer registries' staff and CDC's contractor staff authenticate to the system via user name and password. These user credentials are permanently stored by the system until the project ends.

Save

13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	NPCR-CSS is an external, web-based system which allows CDC to receive de-identified data that will enable public health professionals to understand and address the cancer burden more effectively. NPCR–CSS gives CDC the ability to provide: (1) greater access to cancer data for the public, scientists, and policymakers (national public use data files of cancer incidence); (2) more accurate and more stable estimates of cancer incidence for population groups, including racial and ethnic minorities, medically underserved groups, and other subpopulations; and (3) information for regional and national analyses to more accurately identify geographic variability in cancer treatment practices as a means to assess use of state-of-the-art cancer treatment. NPCR-CSS contains PII information such as name, business email address and phone (used to establish account); user credentials; patient date of birth, state and county of residence; postal code of residence; Census Tract of residence; race/ethnicity; gender; age at diagnosis; and medical information (e.g., cancer patient histology and behavior; ; date of diagnosis; stage at diagnosis; and first course of treatment) .
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 County and postal code of residence Census Tract of Residence user credentials race/ethnicity gender

Save

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?	1,000,000 or more
18	For what primary purpose is the PII used?	Date of birth is used to calculate patient age; cancer incidence and survival are in turn then analyzed by age. Business contact information (name, email address and phone number) is used to set up user accounts.
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).
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: 09-20-0160 Records of Subjects in Health Promotion and Education Studies Published: Published: ☐ In Progress

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.	0920-0469 (06/30/2019)
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.	Each State has a law in place that mandates cancer information reporting to the central cancer registry. State Health Departments routinely collect cancer registry data which includes PII. At the individual central cancer registry level, various mechanisms are in place for notification processes. Notification to individuals of the collection by the State varies, with most states not notifying individuals of the data collection. The Public Health Service Act allows CDC to receive the data without additional notification to the Individuals.
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.	Since each state mandates cancer incidence reporting to the central cancer registry, individuals may not opt-out of the collection or use of their PII. Therefore, no process are in place.
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.	There is no direct interaction with individual patients. However, cancer registry users (i.e., reporting healthcare entities) are notified by email when major changes occur.

Save

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 data is owned by the States. Individual patients are not made aware of CDC receiving the data from the States. Therefore, CDC does not have a process in place. Cancer registry users can contact the CDC project officer if they have concerns in regards to their contact information.	
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.	Patient-level data are de-identified before submission to CDC except for date of birth. Therefore, periodic reviews are not warranted. Contact information for cancer registry users are reviewed annually.	
31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users	upload/download data files
		☐ Administrators	
		☐ Developers	
		☒ Contractors	Developers are contractor staff; Receipt, analysis, and other functions may warrant review of raw data
		☐ Others	
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Access is only granted by the contractor's security steward based on the roles of individuals processing or analyzing those files that contain PII. All users must sign agreements before accessing those files. Security/Confidentially audits are conducted on the system and individuals. USERS: All user accounts are approved by CDC project officers before creation. Registry users only have access to PII they upload to the system. Once uploaded, file(s) in registry specific folders will not be accessible through the web for added security. CONTRACTORS: Contract staff have responsibility for processing and analyzing patient cancer data.	

Save

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 managers, system staff, data analyst, web developer, database administrator, statisticians working on data validation, processing, visualization 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. In addition to that, PII is only available through a process that requires users to sign data use agreements every year before data collection starts.
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.	The contractors that process these data files are trained in standards and procedures to maintain the security and confidentiality of PII. Audits are conducted throughout the year to ensure adherence to these standards. By signing a formal agreement that describes the penalties for failing to observe the security requirements, project members are made aware of the seriousness of project security. The confidentiality agreement at the beginning of each project year, renewing the team member's awareness of security requirements. Security training is conducted periodically and scheduled for the time that project staff renew their confidentiality agreements. The training includes a review of the security requirements and procedures for the project, including relevant portion of the security plan. Project staff are provided with a copy of the security plan at each security training session.
35	Describe training system users receive (above and beyond general security and privacy awareness training).	None.
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 of in accordance with the CDC Records Control Schedule for Scientific and Research Records. Records are maintained at CDC for two years. Source documents are disposed of when no longer needed by program officials. Personal identifiers may be deleted from the records when no longer needed in the study as determined by the system manager, and as provided in the signed consent form, as appropriate.

Save

38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	TECHNICAL: State cancer registries submit encrypted data files to the contractor. Upon receipt, they are encrypted when the files are exposed to the Internet, there is prompt backup to archival media, and there is strict management oversight of all processes to ensure that confidentiality of the data is maintained. PHYSICAL: Computer servers are located in a facility with restricted access. ADMINISTRATIVE: Access is only granted by security steward based on roles of the individuals processing or analyzing those files that contain PII. The contractors that process these data files are trained in standards and procedures to maintain the security and confidentiality of PII. Audits are conducted throughout the year to ensure adherence to these standards. By signing a formal agreement that describes the penalties for failing to observe the security requirements, project members are made aware of the seriousness of project security. The confidentiality agreement at the beginning of each project year, renewing the team member's awareness of security requirements. Security training is conducted periodically and scheduled for the time that project staff renew their confidentiality agreements. The training includes a review of the security requirements and procedures for the project, including relevant portion of the security plan. Project staff are provided with a copy of the security plan at each security training session.
General Comments		
OPDIV Senior Official for Privacy Signature	Beverly E. Walker -S Digitally signed by Beverly E. Walker -S Date: 2018.08.20 16:23:04 -04'00'	