Save

Privacy Impact Assessment Form

v 1.43

Status Draft | Form Number F-43856 | Form Date 9/10/2013 8:15:33 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-7304408-829613
2a	Name:	National Assisted Reproductive Technology (ART) Surveillance S
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: Info Systems Security Officer 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	September 26, 2013 ☐ Not Applicable

Save

11	Describe the purpose of the system.	To collect annual clinic-specific and cycle-specific data from all practicing assisted reproductive technology clinics in the US and its territories.
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.)	NASS collects clinic-specific and cycle-specific data from all practicing assisted reproductive technology (ART) clinics in the US and its territories for the annual successful rates report publishing. This data collection is to fulfill the mandate of the Fertility Clinic Success Rates and Certification Act of 1992. Patients PII are collected with inform consent on voluntary basis prior to the beginning of the treatment.
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The National Assisted Reproductive Technology is a Surveillance System (ART) with an organized infrastructure that enables the ongoing, systematic collection, management, analysis, interpretation, and dissemination of health-related data.
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 Patient zip code, country, city and state of residence patient ethnic background
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?	To determine treatment outcomes from infertility clinics in the United States, and publishes an annual report.

Save

19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	Research
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
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: 09-20-0136 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.	0920-0556, August 31, 2015
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.	Clinics specify in their informed consent that patient data is subject to reporting to CDC.
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.	Patients may decline the informed consent.
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.	No process in place
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.	reasonably identify the record and specify the information being contested, the corrective action sought, and the reasons for requesting the correction, along with supporting information to show how the record is inaccurate, incomplete, untimely, or irrelevant. PII is used for data gathering and analysis only; not used or shared publicly, or obtained for providing services or benefits to individuals or the public.
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 data are validated at the time they are collected, and are used for statistical reporting only. They are maintained in an information system that meets FISMA requirements for safeguarding information confidentiality, integrity, and availability. Assessments are completed annually

Save

31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users	Typical users include analysts, statisticians, research staff, and project senior staff, as well as agency project. The data, which may include IIF, are used for statistical analysis and reporting.
		☒ Administrators	System administrators have access to the structures and hardware supporting the information system containing the IIF. They have access to the data during routine operations such as backups.
		☒ Developers	Developers have access to data stored in databases or data files and/or used for statistical analysis, which may include IIF.
		☒ Contractors	Westat, a contractor, is performing the ART project and operating the NASS information system.
		☐ Others	
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Individuals are granted rights to NASS information by the project director who, in cooperation with the systems manager and other key personnel, determines the need to access PII based on the role the user is assigned and the specific requirements that role requires.	
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 project director's assessment of 'need to know', the network administrator creates and implements network access groups. Examples of such groups would be managers, systems staff, data preparation personnel, help desk staff, statisticians working on data validation 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 subfolder 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 the 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.	All Westat employees are required to annually complete Westat's Information Security Awareness Training which covers all aspects of systems and data security and confidentiality. All systems and network staff must also complete Westat annual contingency plan and disaster recovery training.	

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 shall also receive additional security training as necessary to meet contract requirements. Additionally, all employees assigned to work on the ART project who come in contact with any NASS data are required to review and sign the Contractor's Pledge of 308(d) Confidentiality Safeguards for Individuals and Establishments Against Invasions of Privacy. All systems and network staff must also complete Westat annual contingency plan and disaster recovery 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.	All PII/IIF is stored in a secured IT system or, if on physical media, in locked containers and/or spaces when not in use. Policies and procedures for handling IIF meet FISMA, NIST, HHS, and CDC requirements and guidelines. Upon completion of the contract, all data containing PII are electronically archived and the tapes are securely stored offsite. Westat's standard retention period is three years. The project director determines whether or not to extend the retention period beyond the three years based on contract requirements and/or study specific needs. The archives are destroyed only upon project director 's approval.
38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Information is secured on the system through access controls. Specifically, the NASS application and all other NASS related applications that provide access to PII include strict user authentication, which includes strong passwords that are required to be changed periodically. Access to all databases is restricted to designated internal Westat users and, additionally, native access control features are implemented to further enhance database protection. Furthermore, a comprehensive firewall system with multiple firewalls, routers, and other devices is configured and actively managed to ensure the security of the Westat network infrastructure. In addition to access controls, information is also secured through personnel security awareness and training, regular auditing of information and information management processes, careful monitoring of a properly accredited NASS information system, control of changes to the NASS, appropriate handling and testing of contingencies and contingency planning, ensuring that all users of the NASS are properly identified and authorized for access, and that they are aware of the rules and acknowledge that fact, by ensuring that any incident is handled expeditiously, properly maintaining the NASS and regulating the environment the system operates in, controlling media, evaluating risks and planning for information management and information system operations, by ensuring that the system and any exchange of information is protected, by maintaining the integrity of the NASS and the information stored in it, and by adhering to the requirements established in the contract and statement of work.

Save

	Reviewer Questions	Answer
	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		
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

Save

	Reviewer Questions	Answer
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: 2013.12.17 19:28:02 -05'00'	HHS Senior Agency Official for Privacy