Save

Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-26202 | Form Date: 9/26/2017 1:41:33 PM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-1930569-070768
2a	Name:	National ART Surveillance System(NASS)
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: ISSO POC Name: Cynthia Allen POC Organization: National Center for Chronic Disease Prevention and Health Promotion 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

Save

8b	Planned Date of Security Authorization	July 26, 2018 ☐ Not Applicable
11	Describe the purpose of the system.	National ART Surveillance System (NASS) collects data from every U.S. clinic performing Assisted Reproductive Technology (ART) procedure. NASS is maintained by CDC as a web-based data reporting system that provides a standardized mechanism for ART clinics to fulfill their annual ART data reporting obligation to CDC as required by the Fertility Clinic Success Rate and Certification Act (FCSRCA) of 1992, Section 2(a) of P.L. 102-493 (42 U.S.C.263a-1(a)). NASS enables CDC to publish aggregate ART pregnancy success rate measures in annual reports and surveillance summaries as required by the FCSRCA.
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 information about each ART cycle (i.e., procedure) performed at ART clinics as well as clinic-level profile information that is required per FCSRCA requirements. The categories of cycle-specific data collected for each ART
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	CDC was designated to publish annual reports of ART pregnancy success rates and laboratory certification status by the FCSRCA law of 1992. Consequently, NASS was developed
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 City, State, and/or Zip Code Race/ethnicity ☒ 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

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?	100,000-999,999
18	For what primary purpose is the PII used?	PII is used to determine treatment outcomes from infertility clinics in the United States, and publishes an annual report. PII/IIF data entered into NASS by clinics are maintained in the project information system, and are delivered to CDC annually as part of the NASS cycle-specific dataset for each reporting year.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	NA
20	Describe the function of the SSN.	NA
20a	Cite the **legal authority** to use the SSN.	NA
21	Identify **legal authorities** governing information use and disclosure specific to the system and program.	The Fertility Clinic Success Rate and Certification Act of 1992, Section 2(a) of P.L. 102-493 (42 U.S.C.263a-1(a)).
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

Save

23a	Identify the OMB information collection approval number and expiration date.	OMB Information Collection Approval #0920-0556 Expires 7/31/2018
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.	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.	There is no method for individuals to opt out of the use of their PII because NASS data is not collected directly from individuals; ART programs collect individual information for the purpose of their standard clinical practices. Clinics are then required to report certain data elements in NASS, but only as required by CDC to fulfill FCSRCA requirements. It is noted, however, that other than patient DOB, the NASS reporting system allows for clinics to indicate that the patient refused to provide any information on race, ethnicity, or residency pertaining to each of their ART cycles reported to NASS. Nonetheless, CDC supports providing patients of an accounting of the uses of their information, and many clinics provide patients informational sheets on the uses of their information.
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.	CDC publishes NASS reporting requirements and announces major system changes in Federal Register Notices. The information collected in NASS does not provide identifying information that would allow for notification of individuals if there were changes to disclosure or data; however, the assurance of confidentiality in place prohibits data that are collected in NASS from disclosure.
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.	On the public NASS web page, there are links with information about contacting the NASS Help Desk or CDC with any questions or concerns, about the CDC contracts supporting NASS, about privacy and assurance of confidentiality, about the OMB approval, about the FCSRCA law, as well as links to the Federal Register Notice about reporting requirements. Individuals may also contact the ART clinic that they used for their procedure with any concerns.

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.	NASS data are maintained in an information system that meets FISMA requirements for safeguarding information confidentiality, integrity, and availability. Review of PII accuracy takes place in two stages, NASS embeds logic and skip patterns to generate data alerts for reviewing and confirming of data accuracy during data entry. Additionally, every year approximately 5-10% of the reporting clinics are randomly selected for data validation (35 ART clinics were selected for validation in 2015); this review includes, but is not limited to medical and laboratory records and comparison with data reported in NASS. Finally, NASS data are collected under OMB approval; approvals must be renewed every three years, including a review of the information being collected for its continued relevancy.	
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
		☒ Administrators	System administrators have access to the structures and hardware supporting the information system containing the IIF. They have access to
		☐ Developers	
		☒ Contractors	CDC's contractor performs the ART project and operating and maintaining the NASS information system, and, therefore, requires access to all data
		☒ Others	Clinic staff and medical directors require access to PII to enter/edit all data (including PII). These individuals are not CDC credentialed and only
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	The ART project director is responsible for ensuring that personnel have controlled access only to what is relevant to their specific work on ART. The project director oversees the	
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.	

Save

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 complete Westat's Information Security Awareness Training annually 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. Contract-specific 308(d) assurance of confidentiality training, review of 308(d) contract-specific clause, and annual retraining.
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 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 PII 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 off-site. The current contractor'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. Records are retained, stored, and disposed of in accordance with CDC's Scientific and Research Project Records Control Schedule, http://www.archives.gov/records-mgmt/grs.html. The de-identified datasets are permanent records. No identifiable information will be retained or transferred to the National Archives.

Save

38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Several controls are applied to protect system data. Administrative controls include a security plan, contingency plan, file back-up, least privilege, and training. Technical controls include Usernames and Passwords and a second authentication factor. Physical controls include ID Badges, Key Cards, and Closed Circuit TV (CCTV). Please refer to the Information System Security Plan (ISSP) for further details. Administrative Controls: Access to PII follows a least privilege model. NASS staff receive study specific confidentiality training in addition to IRB training. This training covers the procedures and practices used to protect the confidentiality of the data collected. NASS staff are required at all times to maintain and protect the study data and confidential records that may come into their presence and under their control. This training covers, but is not limited to, the following areas of concern: restrictions on use of information, enhanced protection of computerized files as part of study implementation, dissemination of research results, data sharing with other study partners, analytic data access policies and procedures, instructions concerning confidentiality procedures, procedures for traveling with confidential study materials, loss of study materials containing confidential data. Once confidentiality training is complete, personnel must sign a confidentiality agreement that indicates that signee has carefully read and understands the agreement and the confidentiality of all records handled in regard to NASS. Technical Controls: Access to PII follows a least privilege model. The PII will be secured in NASS. The NASS System Security Plan describes the user privileges and the IRB documents outline who should have access to the PII maintained in the system. Secure logins will be used to prevent unauthorized access from the application. NASS enforces a limited number of invalid access attempts by a user before lockout. Roles will be utilized to prevent unnecessary viewing of PII. Storage will utilize FIPS-compliant encryption. Server room remains locked at all times through the use of RFID key cards and personal security passcodes assigned to individual authorized IT staff with proper security privileges. Physical Controls: Physical measures, policies, and procedures are in place at the contractor's facility to protect information, buildings, and equipment from unauthorized intrusions, environmental hazards, and natural hazards.
General Comments		

Save

OPDIV Senior Official for Privacy Signature	Beverly E. Walker -S	Digitally signed by Beverly E. Walker -S Date: 2018.07.23 09:13:31 -04'00'