Privacy Impact Assessment Form

v 1.21

Status		Form Number		Form Date	

	Question	Answer
1	OPDIV:	CDC/NCHHSTP/DSTDP/SB
2	PIA Unique Identifier:	0920-1072
2a	Name:	Enhanced STD Surveillance Network (eSSuN)
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: Project Officer POC Name: Eloisa Llata, MD, MPH POC Organization: NCHHSTP/DSTDP/SB POC Email: gge3@cdc.gov POC Phone: 404-639-6183
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	☒ Not Applicable

8c	Briefly explain why security authorization is not required	Enhanced SSuN is a surveillance project that does not involve the creation of any electronic applications or utilize any web-based software. Datasets are created locally as individual SAS files and securely transmitted to Division of STD Prevention(DSTDP) with access permissions limited to project officers and 2 data management stewards. Datasets are aggregated in SAS for analysis.	
9	Indicate the following reason(s) for updating this PIA. Choose from the following options.	☒ PIA Validation (PIA Refresh/Annual Review) ☐ Significant System Management Change ☐ Anonymous to Non-Anonymous ☐ Alteration in Character of Data ☐ New Public Access ☐ New Interagency Uses ☐ Internal Flow or Collection ☐ Conversion ☐ Commercial Sources Renewal of existing OMB (0920-1072) eSSuN	
10	Describe in further detail any changes to the system that have occurred since the last PIA.	We are only proposing minor changes to our project (to collect clinical screening information from additional patients with primary/secondary syphilis specifically to assess incidence of neuro/ocular syphilis) but no changes in PII collected, methods or data management processes.	
11	Describe the purpose of the system.	Enhanced STD Surveillance Network (eSSuN) is designed to provide critical clinical, demographic and behavioral information through enhanced and sentinel surveillance among people diagnosed with gonorrhea, early syphilis with ocular/neurologic involvement and those persons seeking care at STD clinics. The objectives of eSSuN are to : 1) assess the prevalence and trends in risk behaviors among persons diagnosed with gonorrhea, 2) enhance STD surveillance data, and inform a more comprehensive understanding of epidemiologic trends and determinants of STDs of interest, 3) monitor public health program impact and provide a more robust evidence-base for directing public health action, and 4) respond to emerging trends in STDs and related behaviors.	

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.)	The Enhanced STD surveillance network awardee's routinely collect PII for the purpose of monitoring persons seeking STD clinic services and contacting individuals with gonorrhea and/or primary & secondary syphilis wtih neuro/ocular manifestations who agree to participate. The information collected at the local/state health department level will include: name, address information, telephone number, date of birth, gender, race/ethnicity, HIV status, sexual behavior, insurance status and type, and medical information such as pre-exposure prophylaxis (PrEP); antiretroviral (ARV) usage, condom usage, and frequency of HIV/STD testing. However, neither names, contact information (eg. address, phone numbers) or date of birth will be provided to CDC; this information will be removed from records prior to being transmitted to CDC as an encrypted file. CDC will only receive and maintain patient age, gender race/ethnicity and nationality. A unique non-identifiable project identification number is assigned to each case. The key to link data will only be available at the local level.
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The Enhanced STD surveillance network utilizes two distinct surveillance strategies to collect information. The first is facility-based STD surveillance which includes abstracting data in a standardized way from each of the 10 sentinel surveillance sites from existing electronic medical records for all patient visits to participating STD clinics during the 3 year OMB time period. The second strategy is population-based STD surveillance where a random sample of reported gonorrhea cases from the total number of gonorrhea case reports received by each jurisdiction are selected and interviewed. Additional information are obtained from passive provider reporting and/or health department record review on the sampled cases including verification of treatment under their local regulatory authority to conduct disease surveillance. Data collected across both strategies include demographic-age, race and gender; behavioral and clinical information-clinic/facility name, medical diagnosis, such as treatment. CDC will only receive and maintain patient age, gender race/ethnicity and nationality. A unique non-identifiable project identification number is assigned to each case. The key to link data will only be available at the local level.
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	Other...
		Other...	Other...
		Other...	Other...

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 only collected pursuant to local legal authority for disease surveillance and used only at the local level to complete case investigations.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	There are no secondary uses.
20	Describe the function of the SSN.	Not applicable- SSN is not collected.
20a	Cite the **legal authority** to use the SSN.	Not applicable-SSN is not collected.
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, "Epidemiologic Studies and Surveilla
		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.	0920-1072; expiration 6/30/2018

24	Is the PII shared with other organizations?	◯ Yes ⦿ No

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)).	Not applicable

24c	Describe the procedures for accounting for disclosures	Not applicable

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.	Project participants are informed that their personal information will be collected prior to their volunteering to participate in the project.
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 have the option to decline to answer any of the interview questions or to participate in the project all together.
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 are no major changes planned for this project. In the event of major changes, the individual project sites have contact information available to notify participants and obtain additional consent if the need arises.
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 should 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. In the event of a suspected data breach, the reporting jurisdiction must report the incident with complete information detailing the nature of the suspected breach to the CDC Project Officer who reports the suspected incident to NCHHSTP's Information Security Office and works with the individual jurisdiction until the matter has been resolved. If, however, the individual believes their PII is inaccurate, this should be reported to the local jurisdiction for further investigation. CDC does not receive or have access to the individual'`s PII.
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.	Data collection requirements as a whole are reviewed by CDC and CDC-funded awardees annually. All PII data is maintained at the local level and not shared with CDC. Review processes may vary as each health department will have jurisdiction-specific guidelines in place for conducting internal reviews of PII in the system. They follow their local data destruction policies regarding any data they may have collected in addition to the final dataset in the course of their routine surveillance activities. They also follow their local policies and procedures for conducting routine reviews of the data to ensure availability, integrity, and access to the data. Accuracy is assured by CDC when they receive the data. CDC receives a final national dataset and maintains these annual datasets on secure data drives at CDC. Annual reviews are conducted to control access and availability of the data to CDC staff. Integrity is ensured by CDC's routine back-ups.

#	Question		
31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users	CDC project officers and data stewards have access to limited PII (e.g., race/
		☐ Administrators	
		☐ Developers	
		☐ Contractors	
		☒ Others	State health department staff collecting the data for eSSuN. The
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Access to PII is based on specific staff role (recruitment, retention, study coordination) based on the established operational protocol for the surveillance project. CDC never has access to the system that is based and managed locally at the state/local health departments for all project sites.	
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.	Enhanced SSuN collection staff at the state/local health departments retrieve only the minimum amount of information required for follow-up data collection for persons who agreed/consented to participate in the interview. Only the project coordination and interviewer and/or network administrators have access to the system containing 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 CDC personnel with data access have completed, and will remain current with, the annual Information Security and Privacy Awareness Training.	
35	Describe training system users receive (above and beyond general security and privacy awareness training).	All local and federal staff with access to eSSuN data receive additional annual security and confidentiality training in accordance with the National Center for HIV/AIDS, viral Hepatitis, STDs, and Tuberculosis Prevention's Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs: Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action. Federal staff's training is audited annually by a review of the signed confidentiality training forms. Anyone without a signed form will have their access to the data systems terminated.	
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 04-4-44c, STD Surveillance Reports, and annual reports. Record copy of study reports are maintained in agency records from two to three years in accordance with retention schedules. Source documents for computer are disposed of when no longer needed by program officials. Personal identifiers may be deleted from records when no longer needed in the study as determined by the system manager, and as provided in the signed consent form, as appropriate. Disposal methods include erasing computer disks or tapes, burning or shredding paper materials or transferring records to the Federal Records Center when 5 years old and offer to NARA when 20 years old.	

38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	The enhanced SSuN awardee's are responsible for following their organizations specific security procedures, which at a minimum include restricting access to the PII to only authorized users. Staff must gain access to the building through a keycard. Authentication for access to the network requires user-id and password. Surveillance data is secured on a network drive protected by a firewall and requiring special access permission for staff through IT health departments.

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		

Reviewer Questions		Answer
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		HHS Senior Agency Official for Privacy	