National HIV Surveillance System (NHSS)

Attachment 7(a).

2015 Privacy Impact Assessment

Save

Privacy Impact Assessment Form

v 1.47.2

Status: Draft | Form Number: F-28686 | Form Date: 9/8/2015 10:37:12 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-9451318-011566
2a	Name:	OID DHAP Enhanced HIV-AIDS Reporting System (eHARS)
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: IT Specialist POC Name: William Dolan POC Organization: NCHHSTP/OD POC Email: lxi4@cdc.gov POC Phone: 404.639.6233
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 19, 2012

Save

11	Describe the purpose of the system.	The OID DHAP Enhanced HIV-AIDS Reporting System (eHARS) system gathers HIV/AIDS data collected by State and Local Health Departments via documents such as case reports, lab reports, death certificates, and birth certificates. This information is used for surveillance and reporting purposes. This data helps CDC answer questions such as how many people are dying from HIV/AIDS in a particular area, whether the death rate is increasing or decreasing, etc.
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.)	Date of Birth, Date of Death (if deceased), City, County, State, Sex, Gender, Race, Ethnicity, and Birth Country.
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The eHARS system is used to collect information about the Nationwide HIV/AIDS epidemic. This data is stored at the State and Local Health Department site level. Each participating
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 ☒ 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 City, County, State Date of Death Birth Country
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?	Public Health Data is shared with NCHHSTP/DHAP/HICSB for surveillance statistical analysis.

Save

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); 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: 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.	0920-0573 9/29/2016

Save

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)).	
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.	The data is received in conjunction with Notifiable Disease Surveillance; it is not originally collected by CDC, but rather forwarded from the State Health Departments who receive it from the individual clinics. It is voluntary that notifiable disease cases be reported to CDC by state and territorial jurisdictions (without direct personal identifiers) for nationwide aggregation and monitoring of disease data.
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.	At the state level, there is no individual consent form or mechanism to opt out of data collection for notifiable disease reporting mandated by state or local law.
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.	Individuals cannot be directly notified as the data is not originally collected by CDC, but forwarded from the State Health Departments who receive it from the individual clinics. Reporting occurs as part of mandated (HIPAA exempt) notifiable disease reporting in each state.
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 individual can contact the System manager (i.e., program manager, business steward), 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.
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.	There are no periodic reviews of the PII contained within the system because there is no method to validate the accuracy or authenticity of the data since the data is received from the State and Local Health Departments.

Save

31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users	Data entry
		☒ Administrators	System Maintenance
		☐ Developers	
		☒ Contractors	Data Analysis
		☐ Others	
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Role-based access controls are used to ensure that only authorized users may access PII.	
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.	The Least Privileged model is utilized	
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.	Annual CDC Security and Privacy Awareness Training (SAT)	
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, 4-23 (HIV/AIDS Surveillance Database). Authorized Disposition: PERMANENT. Transfer a "snapshot" copy of the HIV Surveillance master file to NARA at 5 year intervals, when the newest record is 5 years old. Access restrictions specified under Item 4-22, Family of HIV Surveys, also apply to these records.	
38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	The data is transferred from the State Health Departments to the CDC using two forms of encryption, PGP to encrypt the data at the source and SSL/TLS to encrypt the connection between the State Health Departments and SAMS. There is no encryption on the SQL servers for data at rest. The CDC eHARS and NDP servers are housed in a secure CDC computer room that require building and room electronic access using the individuals Personal Identity Verification (PIV) card. The Chamblee campus has a 24/7 gate guard that requires use of the individuals PIV card and a valid parking sticker to gain access.	
General Comments			

Save

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: 2015.10.22 11:00:58 -04'00'	HHS Senior Agency Official for Privacy	