**National HIV Surveillance System (NHSS)**

Attachment 6(a).

2019 Privacy Impact Assessment

Save

# Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-88964 | Form Date: 1/31/2019 10:30:10 AM

| | Question | Answer |
|---|---|---|
| 1 | OPDIV: | CDC |
| 2 | PIA Unique Identifier: | P-7273719-713935 |
| 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)<br>○ Major Application<br>○ Minor Application (stand-alone)<br>◉ Minor Application (child)<br>○ Electronic Information Collection<br>○ Unknown |
| 3a | Identify the Enterprise Performance Lifecycle Phase of the system. | Operations and Maintenance |
| 3b | Is this a FISMA-Reportable system? | ○ Yes<br>◉ No |
| 4 | Does the system include a Website or online application available to and for the use of the general public? | ○ Yes<br>◉ No |
| 5 | Identify the operator. | ◉ Agency<br>○ Contractor |
| 6 | Point of Contact (POC): | POC Title: IT Specialist<br>POC Name: Carman Layne<br>POC Organization: NCHHSTP/Informatics<br>POC Email: iws6@cdc.gov<br>POC Phone: 770-488-8116 |
| 7 | Is this a new or existing system? | ◉ New<br>○ Existing |
| 8 | Does the system have Security Authorization (SA)? | ○ Yes<br>◉ No |
| 8b | Planned Date of Security Authorization | April 30, 2019<br>☐ Not Applicable |

Save

| | | |
|---|---|---|
| 11 | Describe the purpose of the system. | The Division of HIV/AIDS Prevention (DHAP) Enhanced HIV-AIDS Reporting System (eHARS) system gathers HIV/AIDS 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.) | The information the system collect is: Date of Birth, Date of Death (if deceased), City, Marital status, County, State, Sex, Gender, Race, Ethnicity, Birth Country, Risk factors, Routine |
| 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 ☒ Date of Birth<br>☐ Name ☐ Photographic Identifiers<br>☐ Driver's License Number ☐ Biometric Identifiers<br>☐ Mother's Maiden Name ☐ Vehicle Identifiers<br>☐ E-Mail Address ☐ Mailing Address<br>☐ Phone Numbers ☐ Medical Records Number<br>☐ Medical Notes ☐ Financial Account Info<br>☐ Certificates ☐ Legal Documents<br>☐ Education Records ☐ Device Identifiers<br>☐ Military Status ☐ Employment Status<br>☐ Foreign Activities ☐ Passport Number<br>☐ Taxpayer ID<br>Date of Death/ User Authentication<br>City, County, State<br>username and password<br>Race/ Ethnicity<br>Sex/Gender |
| 16 | Indicate the categories of individuals about whom PII is collected, maintained or shared. | ☐ Employees<br>☐ Public Citizens<br>☐ Business Partners/Contacts (Federal, state, local agencies)<br>☐ Vendors/Suppliers/Contractors<br>☒ Patients<br>Other |
| 17 | How many individuals' PII is in the system? | 1,000,000 or more |
| 18 | For what primary purpose is the PII used? | The purpose of the PII is to help CDC determine how many people are dying from HIV/AIDS in a particular area. |
| 19 | Describe the secondary uses for which the PII will be used (e.g. testing, training or research) | If the death rate is increasing or decreasing. |
| 20 | Describe the function of the SSN. | N/A |

Save

| | | |
|---|---|---|
| 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<br>◉ No |
| 23 | Identify the sources of PII in the system. | Directly from an individual about whom the information pertains<br>☐ In-Person<br>☐ Hard Copy: Mail/Fax<br>☐ Email<br>☐ Online<br>☐ Other<br>Government Sources<br>☐ Within the OPDIV<br>☐ Other HHS OPDIV<br>☒ State/Local/Tribal<br>☐ Foreign<br>☐ Other Federal Entities<br>☐ Other<br>Non-Government Sources<br>☐ Members of the Public<br>☐ Commercial Data Broker<br>☐ Public Media/Internet<br>☐ Private Sector<br>☐ Other |
| 23a | Identify the OMB information collection approval number and expiration date. | OMB No. 0920-0573 expires 06/30/2019 |
| 24 | Is the PII shared with other organizations? | ○ Yes<br>◉ 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. | 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<br>○ 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. |

Save

| | | | |
|---|---|---|---|
| 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, Health Insurance Portability and Accountability Act (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. | If an individual has concerns that their PII has been inappropriately obtained, used or disclosed, they will contact their State and Local Health Departments, HIV Surveillance Programs for assistance. | |
| 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. | |
| 31 | Identify who will have access to the PII in the system and the reason why they require access. | ☒ Users | Will have access to their PII for matching HIV cases, initiate a HIV case investigation and for required HIV |
| | | ☒ Administrators | Local state health department eHARS database for system maintenance. |
| | | ☐ Developers | |
| | | ☐ Contractors | |
| | | ☐ Others | |
| 32 | Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII. | The State and Local Health Departments HIV surveillance program coordinator determines which staff members may use the eHARS system, based on the staff member's roles and | |
| 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 privilege model is utilized to allow those with access to PII to only access the minimum amount of information necessary to perform their job. | |
| 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. | CDC personnel are required to complete the annual OCISO Security Awareness Training (SAT) to make them aware of their responsibilities for protecting the information being collected and maintained. | |
| 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<br>○ 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. | |

Save

| | | |
|---|---|---|
| 38 | Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls. | Administrative:<br>CDC will not receive or store PII. All State and Local Health Department staff collecting data will participate in a training that will review protections for privacy and confidentiality of all data, including PII.<br><br>Technical:<br>The data is transferred from the State Health Departments to the CDC using two forms of encryption, Pretty Good Privacy (PGP) to encrypt the data at the source and Secure Sockets Layer (SSL)/Transport Layer Security (TLS) to encrypt the connection between the State Health Departments and SAMS.<br><br>Physical:<br>The CDC eHARS and National Data Processing (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 | | |
| OPDIV Senior Official for Privacy Signature | Jarell Oshodi -S | Digitally signed by Jarell Oshodi -S<br>Date: 2019.04.10 16:10:17 -04'00' |