Save

Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-62894 | Form Date: 5/11/2022 8:28:57 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-1792400-970349
2a	Name:	Web-based Integrated Surveillance Management System (WISMS)
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.	Development
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: Carman Layne POC Organization: NCHHSTP/OD POC Email: iws6@cdc.gov POC Phone: 770.488.8116
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	July 15, 2022 ☐ Not Applicable

Save

11	Describe the purpose of the system.	The web-based surveillance management system (WISMS) with off-line capability will provides project sites with real-time/near real-time data collection, data linkage, data validations, and data quality checks. The system will be used to support HIV surveillance activities at the Medical Monitoring Project (MMP) and National HIV Behavioral Surveillance (NHBS) operational sites/locations. WISMS will have extensive automated data acquisition mechanisms that can be reused. The automation and integration of the data acquisition will eliminate many manual steps currently used in data management processing.
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 types of data WISMS stores from NHBS and MMP area sites are: birth-date, sex at birth, year of birth, birth county, gender, race, ethnicity, zip-code and MMP Participant ID (ParID). The ParID contains a list of de-identified field variables about the person's (Public Citizen) disposition which are: interview date, interview status, date of first contact and attempts, lead source, data collector IDs, user-name of person syncing and time. Data sets are then returned to the project area sites to use for their local analysis and reporting the national HIV database. External user access to this application is authenticated via the Secured Authentication Management System (SAMS) authentication. (CDC) user access is authenticated via Personal Identity Verification (PIV) and Active Directory (AD). Both SAMS and AD are separate systems with their own, individual Privacy Impact Assessment (PIA).

Save

13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The web-based surveillance management system (WISMS) with off-line capability will provides project sites with real-time/near real-time data collection, data linkage, data validations, and data quality checks. The system will be used to support HIV surveillance activities for Medical Monitoring Project (MMP) and National HIV Behavioral Surveillance (NHBS) System sites. The purposes of this system is to: 1. Maintain and update the existing data portal to provide seamless support to the collection and management of NHBS and MMP data; 2. Provide a web-based integrated surveillance management system and supporting modules that replace legacy data collection instruments currently in use by MMP and NHBS; 3. Produce high quality, timely data sets ready for analyses and public health action; and 4. Provide operational and technical supports to MMP and NHBS projects. Types of data WISMS stores from NHBS and MMP area sites are; birth-date, sex at birth, year of birth, birth county, gender, race, ethnicity, zip-code and MMP Participant ID (ParID). The ParID contains a list of de-identified field variables about the person's (Public Citizen) disposition which are: interview date, interview status, date of first contact and attempts, lead source, data collector IDs, user-name of person syncing and time. Data sets are then returned to the project area sites to use for their local analysis and reporting the national HIV database. External user access to this application is authenticated via the Secured Authentication Management System (SAMS) authentication. (CDC) user access is authenticated via Personal Identity Verification (PIV) and Active Directory (AD). Both SAMS and AD are separate systems with their own, individual Privacy Impact Assessment (PIA).
14	Does the system collect, maintain, use or share **PII**?	(•) Yes ( ) No

Save

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 Zip codes year of birth, race/ ethnicity gender/sex at birth birth county MMP Participant ID (ParID): interview date, interview status, date of first contact and attempts, lead source, data collector IDs, user-name of person syncing and time
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?	Person (Public Citizen) PII will be used for surveillance and reporting of cumulative HIV data to CDC.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or 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)).

Save

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
23a	Identify the OMB information collection approval number and expiration date.	N/A
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.	Not applicable. Notice is the responsibility of the state and local health departments and HIV Surveillance Programs that originally collect the information and provide it into the subject system.
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.	The method at the local, state level, individuals have the option to decline to answer any of the interview questions.
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.	It would not be possible to notify individuals because the system does not process data that would enable contacting individuals. Any contact with individuals would be the responsibility of state and local health departments, HIV Surveillance Programs collecting and providing the data in this system.
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.	Not applicable. Collecting the data and resolving individual concerns are performed by the state and local health departments' HIV Surveillance Programs.

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.	The process involves security/privacy reviews that are conducted annually by National Center for HIV/AIDs, Viral Hepatitis, STD & TB Prevention (NCHHSTP) security stewards to determine access and availability of the data to CDC users is in-place. Integrity is ensured by CDC's routine back-ups.	
31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users	(User) need access to real-time/near real-time data collection, data linkage, data validations.
		☒ Administrators	Administrators need access to update and improve the system and applicable tools. They also perform dataset reviews and reporting.
		☐ Developers	
		☒ Contractors	(Direct Contractors) are administrators and need access to update and improve the system and applicable tools. They also perform dataset
		☐ Others	
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	There are two roles in WISMS, admin, and user. The admin role determines who has access to PII through access control list (ACL). Role-based access controls (RBAC) are configured so that each user could access only the data necessary for the user's role. User roles only access (Public Citizen) data they input.	
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 ensure those with access to data only have access to the minimum amount of data assigned to them by access-level (i.e., read, write, full) 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/Direct Contractor): Annual CDC Security and Privacy Awareness Training (SAT) is required. Project sites are required to complete their organization specific Security Awareness training.	
35	Describe training system users receive (above and beyond general security and privacy awareness training).	N/A	
36	Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?	◉ Yes ○ No	

Save

37	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.	Internal (CDC users) are required to use the CDC Records Control Schedule. The applicable section is General Records Schedule (GRS) 4.2: Information Access and Protection Records which states destruction when 3 years old, but longer retention is authorized if needed for business use. Information that would permit identification of any individual or establishment is collected with a guarantee that it will be held in confidence, will be used only for purposes stated in reporting forms, and will not be otherwise disclosed or released without the consent of the individual or the establishment in accordance with Sections 306 and 308(d) of the Public Health Service Act (42 USC 242K and 252m, {d}). Access to the data set is limited to members of the Division of HIV/AIDS performing activities or analysis supporting public health activities. Appeal is to the Director, Division of HIV/AIDS, National Center for HIV/AIDs, Viral Hepatitis, STD & TB Prevention (NCHHSTP), or Director, CDC. CDC doesn't access the PII, CDC data sets are encrypted when submitted to the Data Portal. No information will be disclosed to the public, parties involved in civil, criminal, or administrative litigation, or non-public-health agencies of the federal, state, or local government. Retention and destruction of (Public Citizen) data process is handled by their state and local health departments, HIV Surveillance Programs.	

Save

38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Administrative: The System Security Plan (SSP) documents the system's in-place security controls. A business continuity plan exists for the system. Regular backup of critical files and databases are performed as required by CDC. The project area sites are responsible for following their organization specific security procedures, which at a minimum include restricting access to the PII to only authorized site users. CDC users are required to follow CDC and HHS, policies and procedures for protecting PII information. This includes restricting access to PII following approved access control list (ACL). Annual CDC Security and Privacy Awareness Training (SAT) is required. Technical: Office of the Information Officer (OCIO) Azure General Support System (GSS) and WISMS users authorized access through SAMS authentication. Two-factor authentication is in use for remote access to system servers. IP address restrictions are in place for access to server network ports. (Public Citizen) data in-transit occur over an approved encrypted protocol. Firewalls and Intrusion Detection Systems are deployed on the network, which limit connections to the system and report anomalous traffic. The application utilizes role-based access controls. Physical: Azure Cloud: CDC is dependent upon Microsoft policy and procedures in its data centers. The building hosting the system servers requires PIV card access 24/7. All CDC facilities are camera monitored 24/7. Furthermore, Application Hosting Branch (AHB) server rooms are climate-controlled, have Uninterrupted Power Supply protection for systems, and cameras that send images to the Digital Services Office (DSO) personnel.
General Comments		
OPDIV Senior Official for Privacy Signature	Beverly E. Walker -S Digitally signed by Beverly E. Walker -S Date: 2022.05.25 12:00:55 -04'00'	