Save

Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-87704 | Form Date: 7/25/2017 8:18:17 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-7106604-395613
2a	Name:	Discovere Registries (HOPS)
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: Security Steward POC Name: Mwiche Longa Kaira POC Organization: NCHHSTP/OD POC Email: nnh8@cdc.gov POC Phone: 404.639.8508
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 27, 2018 ☐ Not Applicable

Save

11	Describe the purpose of the system.	The HOPS system is used to monitor trends in the demographics (e.g. age, sex, race, ethnicity), symptoms (e.g. of any illness), diagnoses (e.g. HIV related/Non-HIV related), and treatments (e.g. HIV related and Non-HIV related) in a population of HIV-infected outpatient clinics in five cities. The system helps to describe how to improve medical management of HIV infection in the United States. CDC Epidemiologist use data to study factors associated with clinical, immunologic, and virologic successes for HIV infected patients such as reduced mortality, and emerging issues with long-term HIV infection and the treatment. The data is collected by the Cerner Corporation for a cohort of HIV-infected outpatient adults receiving care at HIV specialty clinics in Denver, Chicago, Philadelphia, Stonybrook and Washington DC. The HIV Outpatient Study (HOPS) utilizes collected data in the existing electronic charting systems of participating clinics, and combines and harmonizes these data in a centralized application, to obtain a complete record of prospective outpatient visits to leading HIV clinicians.
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 HOPS data is collected from HIV-infected outpatient adults receiving care at HIV specialty clinics in: Denver, Chicago, Philadelphia, Stonybrook and Washington DC. The medical record abstraction data is on demographics, risk factors,
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The objectives of the HOPS are to: HOPS data will be used to develop guidelines and recommendations for clinicians, public health departments, and other partners participating in the
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 Name and DOB are required to participate in the study as well as sex, race, ethnicity, and gender. The other fields collected are optional.

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?	500-4,999
18	For what primary purpose is the PII used?	The PII primary purpose is to monitor trends in the demographics, symptoms, diagnoses, and treatments in a population of HIV-infected outpatient clinics across the United States.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	The secondary uses of the PII: (1) Describe factors associated with clinical, immunologic and virologic successes, as well as improved survival, (2) Characterize (new) problems associated with long-term HIV infection and its treatment and (3) Describe HIV risk behaviors and other risk behaviors (e.g., tobacco use, adherence to antiretroviral therapy) among HIV-infected patients.
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, Title III, Section 301
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: SORN 09-20-0160, "Records of Subjects in Health Promotion and Education Studies" Published: Published: ☐ In Progress

Save

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.	OMB No. 0920-1080, exp. 08/31/2018
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.	Patients are approached by HOPS project clinic staff during one of their routine clinic visits and invited to participate in the HOPS. Patients, who have been actively recruited throughout the study period for this ongoing project, sign informed consents to have information collected from their physician visits. The privacy section of the informed consent states that "Your personal identifying information (including your name, date of birth, and possibly your medical record number) will be entered and kept in a private and secure database, separately from your medical information".
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.	Patients recruited to participate in HOPS by their physicians are provided with a consent form discussing the specifics of the study. Persons electing to participate in the study sign a copy of the consent form to be kept on file with the study site and they are also given a copy to keep. The HOPS is completely voluntary. Patients who are approached and decline participation in the HOPS are excluded from enrollment and data collection. Because this is a voluntary collection, respondents are free to withdraw from the study at any time. Patients can withdraw at anytime from study either verbally or in writing to either the study coordinator or physician.

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.	Should "major" changes occur, patients participating in the HOPS would be notified by study staff at the site of their enrollment and of these changes and then given the option to be re-consented indicating their acceptance of these changes or discontinue their participation.
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.	HOPS participant would be notified by study site principal investigator if their PII has been "inappropriately obtained, used, or disclosed". The patient will then be given the option to remain in or withdraw from the study.
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 contractor is required to perform annual review visits at each study site and abstracted data such as name and DOB are evaluated for integrity and accuracy by comparing the abstracted information to data contained in the original medical record.
31	Identify who will have access to the PII in the system and the reason why they require access.	☐ Users ☐ Administrators ☐ Developers ☒ Contractors: For data analysis purposes ☒ Others: CDC HOPS project personnel for data analysis purposes
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	All accounts created for the design and maintenance of the HOPS are approved by the HOPS Research Project Leader (RPL) with the exception of the Discovere master system
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.	Discovere requires each system user to have a unique log-in ID and a private password. Users must enter their log-in ID and password each time they access Discovere. Discovere uses a role-privilege based access model where each role is comprised of a set of permissions. Each permission allows access to particular functions or areas of the Discovere web site. Access to system features and the corresponding study information is restricted based on the roles associated with each log-in ID. Only a user with the system administrator role can change a user's role or make changes to the list of permission associated with a user's role. All users for the HOPS are personally known to the Cerner Research Project Leader assigned to HOPS.

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.	Collaborative Institutional Training Initiative (CITI) training and or Office for Human Research Protections(OHRP) are required for individuals interacting with participants and entering data. Security and Privacy Awareness training is required for associates who may need to access the data base to troubleshoot, update, work on the Discovere database. This is required before allowing access to Discovere and a log is kept with training expiration dates.	
35	Describe training system users receive (above and beyond general security and privacy awareness training).	Collaborative Institutional Training Initiative (CITI training) training and/or Office for Human Research Protections (OHRP training) are required for individuals interacting with participants and entering data.	
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 04-4-22 Family of HIV Surveys, Division of HIV/AIDS Prevention/Surveillance and Epidemiology, (N1-442-02-3-4, Item 1) and Division of HIV/ AIDS Prevention/Surveillance and Epidemiology, (N1-442-02-3, Item 1). 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 no longer needed for evaluation and analysis. Cut off closed grant, contract, or cooperative agreement files at the end of the calendar year in which the project ends or a final report is written and destroy six years after cut off.	

Save

38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Technical All PII pulled from the participant's medical record is stored electronically in the Discovere database. Roll based access, password protected workstations, database "time-outs" after amount of idle time protect the stored PII. Unique user account IDs are issued to all end users and they are instructed to not share account information, passwords, or keep paper copies of log-in information. Administrative Discovere acounts are disabled after 6 failed attempts to log in and user must call project team to enable account again. Cerner project team members are familiar with all end users because it is a relatively small group. Role-based permissions allow users to only perform tasks within the database that are associated with their assigned role. Site level access ensures end users are only able to view/edit data from participants at their assigned site. User passwords expire after 30 days. Physical Physical copies of the signed informed consents are kept in a secure location at each site. This physical security is verified at the annual review visit. Cerner's facility has a 24x7 security presence to ensure protection of PII. Cerner employs physical and electronic patrol/access to location. Multiple access points must be crossed to access the data center floor. Cerner utilizes multiple overlapping security applications or countermeasures to provide greater security. All security solutions work in conjunction to create a holistic security model and support strategy. Administrative access to the data centers is allowed only by VPN and all connections are tracked and logged. External application access across public networks is protected by encryption. All network devices, security infrastructure components, and server systems transfer logs to a centralized repository for analysis, troubleshooting, compliance, and auditing purposes.
	General Comments	
	OPDIV Senior Official for Privacy Signature	Beverly E. Walker -S Digitally signed by Beverly E. Walker -S Date: 2018.07.19 16:33:17 -04'00'