Save

Privacy Impact Assessment Form

v 1.21

Status | Form Number | Form Date 02/22/23

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	0920-23AQ
2a	Name:	Understanding HIV/STD Risk and Enhancing PrEP Implementatio
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.	Initiation
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 Coordinator POC Name: Patricia Bessler POC Organization: NCHHSTP/DHP/HRB POC Email: vey4@cdc.gov POC Phone: 404.639.8239
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

Save

8c	Briefly explain why security authorization is not required	TBD
10	Describe in further detail any changes to the system that have occurred since the last PIA.	N/A
11	Describe the purpose of the system.	The purpose of the activity is to collect and store data for the "Understanding HIV/STD Risk and Enhancing PrEP Implementation Messaging in a Diverse Community-Based Sample of Gay, Bisexual, and Other Men Who Have Sex with Men in a Transformational Era (MIC-DROP)" study, funded by the Centers for Disease Control and Prevention under cooperative agreement #U01PS005244. 1275 participants will be enrolled in a study designed to develop knowledge about PrEP use and adherence. Data from quantitative assessments, in-depth interviews, and focus group will be used to collect information.
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.)	Data to be collected will include eligibility data (screening), consent to participate, contact information, and biological specimens for HIV and STI testing. Participants will also be asked to download the SMaRT application on their mobile phone. The SMaRT app supports key functions including notifications, reminders, messages, survey administration, and appointment scheduling. PII, specifically name, will be included on the screener, consent forms, and the linking document which links a unique participant ID to a participant. Name, email address, telephone number, and mailing address will be included on the locator form. Data of birth and employment type, including military, will be collected in the quantitative surveys. IP address will be gathered during the online data collection process. Name, email address, telephone number, IP and mailing address will not be reported and will not be shared with CDC. Participant date of birth (DOB) and individual employment type will not be reported. DOB will be transformed to age during the analysis. Only aggregated age and employment type will be reported.

Save

13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	All online survey data will be collected using Alchemer, a HIPAA compliant, encrypted electronic platform. Collected data are automatically encrypted, with coded access only available through the Data Manager and the Principal Investigators. Study data stored by Alchemer are maintained on a dedicated secure server. All web survey data will be secured using an SSL 256-bit encryption. Assessment, interview, focus group, and biospecimen data files will be identified using numeric participant ID numbers unrelated to the participant's PII. Study data and personal information will be secured with role-based security. Participants will have the option of completing their focus group or in-depth interview either in person or over a HIPAA-compliant video server. Focus groups and interviews will be digitally audio-recorded. Recorded information will be deidentified during the transcription process. Recordings and transcripts will be stored on a secure computer. Audio recordings will be destroyed 2 years after the end of the study. Data collected through the SMaRT app will be stored on a secure, HIPAA-compliant server housed at Emory University on an Emory AWS RDS database using in-box AWS database encryption. Data in transit will be encrypted with TLS 1.2. The study team will not be able to access participants' mobile device activity, they will only be able to see their completion of some activities in the study app through its admin web portal. Participants will be required to log in to the application with a username and password. Data are stored on the server and not locally in the app. Per HIPAA requirements, sessions expire after several minutes and require users to log back in. When participants finish the study, we will help them remove the app from their mobile device and they will no longer be able to log in to the app. CDC will not receive PII; all data received will be de-identified. Six months after study completion, participant contact information and all links between participant PII and participant number will be destroyed. De-linked study data will be retained by Emory University for up to 25 years after study closure.
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 IP addresses will be collected for internal auditing purposes only (to identify fraudulent or duplicate web entries). 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?	500-4,999
18	For what primary purpose is the PII used?	Name, e-mail, phone number, and mailing address will be used to maintain and track the participants throughout the study. Name and e-mail address will be used to reimburse participants (incentives) and for internal auditing purposes. Mailing address will be used to ship biospecimen collection kits to participants. IP addresses will be used only for the purposes of identifying fraudulent or duplicate web entries and authenticate unique trial participants to protect the integrity of the sample and trial results. Name, email, phone number, IP and mailing address will not be shared with CDC.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	DOB and employment type (including military) will be aggregated and used in the analysis. Only aggregated data will be reported.
20	Describe the function of the SSN.	N/A No social security numbers are being collected.
20a	Cite the **legal authority** to use the SSN.	N/A

Save

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
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.	New ICR not yet approved.
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.	Prior to data collection, participants will be notified in writing (in the consent form) during the consent process that their personal information will be collected.
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.	Participants may opt out of the information collection during either the screening or consent processes. Participants may voluntarily withdraw from the study and end data collection for any reason at any time.
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.	Participants may be notified in writing by study staff if major changes occur to the system.

Save

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.	Participants will receive contact information for the principal investigator as well as the Columbia University Institutional Review Board (IRB).	
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.	We will adopt a Data and Safety Monitoring Plan. Staff will be trained in data collection procedures. All study staff will be trained to recognize, document, and report any unusual events or circumstances that occur during data collection immediately to the PI and Emory IRB. The Principal Investigators and Project Director will monitor staff closely. Staff deficient in any aspect of performance will be re-trained or terminated. Ongoing data monitoring will be conducted by the lead study investigators and project directors throughout the study. In addition, the primary IRB of record will conduct regular reviews of study protocols, changes in study protocols, and adherence to protocols in the field. The lead study investigators are required to report any unexpected study-related adverse events to the IRB and CDC.	
31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users ☐ Administrators ☐ Developers ☐ Contractors ☐ Others	Only research staff will have access to PII in the system in order to collect
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Study content will be secured using role-based access. Access to PII will be restricted to the Principal Investigators; the Retention Coordinator, who must contact participants to schedule visits; the Study Director and Coordinator who will notify participants about test results; study staff who will distribute and audit study tokens and confirm participant web identity; and 3 graduate research assistants who will perform data entry.	
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.	Access to sensitive Personally Identifiable Information (PII) will be restricted to individuals trained in human subject protections who are listed on the Institutional Review Board (IRB) protocol. All PII is collected for a specific and identifiable purpose with access restricted to specific job tasks and individuals who perform those tasks. Access to PII in study data collected for the purposes of analysis is limited to the study investigators and data manager.	
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 study personnel will have completed training and received certification in Human Subjects Research Protection (CITI). These trainings will be renewed in compliance with institutional policies.	
35	Describe training system users receive (above and beyond general security and privacy awareness training).	All study staff will be trained to recognize, document, and report any unusual events or circumstances that occur during data collection immediately to study managers and the IRB.	

Save

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.	Six months after the study is completed, study ID numbers for all participants will be de-linked from contact information in the participant database. De-linked study data will be retained for up to 25 years in accordance with Emory University Libraries and Information Technology Records Management Policy, Policy #5.21, Research Records: Clinical Trials, 21 CFR 312.62 (c); O.C.G.A. 9-3-24; (updated 10/1/2022). All data shared with CDC will be stripped of PII. De-identified study data received by CDC will be retained 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). Data will be archived according to guidance set forth by CDC Records Management Policy, Policy # CDC-GA-2005-07 (updated 9/14/2021).
38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Physical Controls: Consents and contact information paper forms will be stored in locked cabinets in the research offices at Emory University. The servers are located in a secure area with all appropriate physical security measures in place. Technical Controls: The intervention content, questionnaires, and personal information will be secured with role-based security that will provide different types of users with different access privileges. Data containing unique identifiers and data containing the participants' ID number will be maintained separately on the secured server. A master list linking unique identifiers and data will be stored separately, and access to these confidential files will be limited to the Study Director and Principal Investigators. Participant data will be stored by Alchemer on a secure, HIPAA-compliant webserver in a secure database within Emory's firewall. Focus groups and interviews will be digitally audio-recorded and de-identified during the transcription process. Data collected through the SMaRT app will be stored on the HIPPA-compliant server at Emory University. All electronic files and records will be stored in a firewall-protected Emory AWS RDS database using in-box AWS at Emory University. Data in transit will be encrypted with TLS 1.2. The web and database servers are monitored by Emory University IT staff, patched frequently, and scanned by a third-party vendor to ensure that they are protected against known vulnerabilities. The data is backed up to electronic media daily. The electronic media is secured and stored in a secure area separate from the servers. Administrative Controls: The Study Research Staff are responsible for following their organization's specific security procedures, which at a minimum includes restricting access to the PII to only authorized users. Assessment, interview, focus group, and biospecimen data files will be identified using numeric participant ID numbers unrelated to the participant's PII. All study data are only accessible by trained study staff and password protected.

Save

Reviewer Questions		Answer
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		
9	Is applicability of the Privacy Act captured correctly and is a SORN published or does it need to be?	( ) Yes ( ) No
Reviewer Notes	N/A	
10	Is the PII appropriately limited for use internally and with third parties?	(•) Yes ( ) No

Save

	Reviewer Questions	Answer
	Reviewer Notes	
11	Does the PIA demonstrate compliance with all Web privacy requirements?	◯ Yes ◯ No
	Reviewer Notes	N/A
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	Beverly E. Walker -S Digitally signed by Beverly E. Walker -S Date: 2023.04.04 14:56:26 -04'00'	HHS Senior Agency Official for Privacy	