Save

Privacy Impact Assessment Form

v 1.21

Status | Form Number | Form Date 03/13/23

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	TBD
2a	Name:	mChoice: Improving PrEP Uptake and Adherence among Minori
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: Physician POC Name: Mary Tanner POC Organization: NCHHSTP/DHP/HRB POC Email: klt6@cdc.gov POC Phone: 404.639.6376
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 system is to collect and store data for the mChoice research study. The information collected through this study will be used to: 1) improve the overall pre-exposure prophylaxis (PrEP) experience of providers and men who have sex with men (MSM) patients by implementing evidence-based education and support tools in clinical settings; and 2) increase our understanding of provider and patient factors that influence the choice of PrEP regimen by MSM in New York City (NYC), New York (NY) and Birmingham, Alabama (AL). Findings from the data collected during this study will be used to support expanded use of effective provider PrEP tools and increase understanding of PrEP use by MSM to inform the future revisions of CDC PrEP recommendations and interventions to increase PrEP use by persons in priority populations.

Save

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.)	400 participants will be enrolled in a study to assess the effectiveness of the mChoice clinical intervention to increase PrEP adherence and persistence among young MSM using PrEP. Serial assessments and interviews will be used to collect information that will be used to assess attitudes, knowledge, behavior, and experiences related to PrEP and risk factors for HIV acquisition. Other data to be collected will include eligibility (screening) data, consent to participate and contact information (locator form). Participants medication bottles will be fitted with a CleverCap and participants will download the accompanying CleverCap app to their mobile phones. CleverCap collects information about participant medication adherence. In addition, PrEP clinical care data will be collected from electronic medical records to further assess medication adherence. PII, specifically name, will be included in the eligibility screener, consent forms, and the linking document which links a unique participant ID to a participant's name. Contact information, specifically name, email, telephone number, and mailing address will be collected on the locator form. This information will be used for the purposes of participant scheduling and retention throughout the 18-month follow up period. Participant DOB and employment status data will be collected on the baseline survey form. Age and Employment type will be aggregated and used in the analysis. Only aggregated age and employment type will be reported. For healthcare providers, job role (employment type) will be collected on the eligibility form. This information will be used to confirm that the participant meets study eligibility criteria (a PrEP provider at one of the four participating clinics). Job role will be aggregated and used in the analysis. Only aggregated information about job roles will be reported. Electronic health records (EHR) will be reviewed to gather PrEP clinic care data and urine specimen data. These data will be used to evaluate PrEP adherence and persistence. Only study staff will have access to PII. The funded recipient (Columbia University) will be responsible for data collection and management. CDC will not collect nor manage data. CDC will not have access to PII. Prior to securely transferring study data to CDC, Columbia University will strip all PII from the data.
		Patient and provider respondents will complete computer-assisted self-administered web assessments on their computer, phone, or tablet using a secure data collection platform, REDCap, hosted by Columbia University Irving Medical Center (CUIMC) Information Technology (IT). REDCap is a secure web-based system that provides an intuitive interface, audit trails, and automated export. Staff at each site will have a link to the secure web-based data collection survey tool and will be present to assist participants in completing surveys. Data will be stored using REDCap at each respective performance site, encrypted data will be transferred to CUIMC and then the de-identified data will be stored on secure HIPAA-compliant servers at the CUIMC campus. Access to individually identified private information about human subjects will be limited to research team members who collect and manage the data, study staff, site principal investigators and the Principal Investigator. The material, records, and data obtained through participation in the study will be specifically for research purposes. All surveys, case report forms (CRFs), and other study records will be identified by a coded number (a participant identification number), and

Save

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 Age Other... ☒ 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 Employment status Employment type/job role 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?	100-499
18	For what primary purpose is the PII used?	Name, phone number, mailing address, and e-mail address will be used only for the purposes of participant scheduling and retention. PII will be stripped from data shared with CDC. Medical notes (electronic health records [EHR]) will be accessed to retrieve PrEP eligibility, PrEP adherence, and STI and HIV test result data.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	Date of birth and employment status will be aggregated and used in the analysis. Only aggregated age and employment type will be reported. No PII will be shared with CDC.
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
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
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.	New ICR not yet approved
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)).	

Save

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.	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 who are eligible and interested in participation will be enrolled and consent obtained during either the screening or consent processes. Enrollees may end their study participation 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. Notifications will be signed by the study Principal Investigator (grantee) and include contact information if study participants have questions or concerns. CDC will be notified in advance about any proposed changes to the study and any notifications sent to study participants.
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 be provided contact information and instruction to contact the grantee Principal Investigator and 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.	Biweekly reports for the study sites will be created by the data manager to review relevant app engagement data, barriers with recruitment/enrollment and retention, laboratory and medical records, compliance with the protocol, and accuracy and completeness of the records. The investigative team will schedule biweekly conference calls, and these reports will be briefly reviewed by the team at these meetings. These regular reviews will ensure close communication between the research assistants, quickly identify missing data points, and ensure consistent management of any issues with the protocol across sites. Data quality will be examined before statistical analyses are conducted, including examination of missing data, assessment of distributional assumptions, and identification of outliers. In addition to data quality, the comparability between intervention and control groups will be carefully examined, including baseline balance and differential attritions at all waves of follow-up. Ongoing monitoring will be conducted throughout the study by the PIs and Data and Safety Monitoring Board. In addition, the Columbia University IRB (as prime IRB) will conduct regular reviews of study protocols, changes in study protocols, and adherence to protocols in the field. Project PIs are required to report any unexpected study-related adverse events to the IRB and CDC.

Save

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.	Only the research study team will have access to study data. No other individuals will have access. REDCap accounts are password protected. Data will be stored on secure, HIPAA compliant, password protected, servers at Columbia University. Data collection and management, and analysis will be carried out by the funded recipient (Columbia University). CDC will not receive nor have access to 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.	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.	
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.	Columbia University staff receive introductory information and regular notices concerning their responsibilities to follow security protocols and protect information stored on University servers.	
35	Describe training system users receive (above and beyond general security and privacy awareness training).	Training for all staff includes (but is not limited to) Human Subjects Research Protection, Informed Consent, Good Clinical Practice, Quality Management, Confidentiality, and Reporting of Adverse Events.	
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.	All data will be retained by the Columbia University Research Team until analyses are complete and for up to three years following study closure, in line with Columbia University IRB guidelines. Study closure date will be determined by 1) final reporting to the research sponsor; 2) final financial close-out of a sponsored research award; 3) final publication of research results; or 4) cessation of an academic or research project, regardless of whether its results are published. At that time, users must delete all data stored on their servers. At the end of the study, study data shared with CDC will be stripped of PII by the funded recipient Columbia University. De-identified study data will be sent to CDC via secure file transfer. De-identified 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 Paper forms will be stored in locked cabinets in the research offices. Study records will be recognized by a participant ID number and stored in password-protected files on secure servers. All laboratory specimens will be identified only by the identification number. The code linking the participant identification number to subject identifying information (name, address, etc.) is maintained at the clinical sites through REDCap, and only authorized site personnel have access to the code. The code will be destroyed two years after publication of study findings. Technical RedCap, a HIPAA-compliant web-based platform, will be used for data capture and storage. RedCap is supported by Columbia University. Standard features of RedCap include interactive data entry with real-time field validation, lab data imports, audit logs to record database modifications, database integrity checks, security (in logins, permissions based on need, and encryption), reporting, forms inventory, and exports to common statistical packages for analysis. Logging tracks all data entered in REDCap so that it can be traced back to the person who entered it. No data can be changed without showing who has made the changes. This allows the study team to ensure the security and integrity of the data collected and submitted; therefore, there are controls surrounding this aspect. REDCap also provides for principal investigator sign-off on data, as required in FDA studies. Although users can modify data based on their permissions, they cannot delete the subject or history of that subject. Requests to delete a subject must be made to the REDCap system administrator. RedCap database system provides for secure web-based data entry with the data stored on servers maintained by Columbia University IT. The data is encrypted during transmission. The servers are located in a secure campus area with all appropriate physical security measures in place. The web and database servers are monitored by University IT staff, patched frequently, and scanned to ensure that they are protected against known vulnerabilities. Access is by individual user ID and is restricted to the forms and/or functions that the user needs to have. The data is backed up to electronic media daily. The electronic media is secured by IT staff and stored in a secure area separate from the servers. Administrative Controls: Participants are assigned a unique identification number. Unique identifiers for each participant will be a combination of letters and numbers. The letters will be "MCH," short for "mChoice" and the number will indicate what order the participant was enrolled in the study. For example, the first participant will be "MCH001”. Documents with participant’s names or other identifying information (such as informed consent forms) will be stored separately from other study documents and only research project staff will have access to it.

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		
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		
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	Jarell Oshodi -S Digitally signed by Jarell Oshodi -S Date: 2023.04.25 18:43:31 -04'00'	HHS Senior Agency Official for Privacy	