Save

Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-52108 | Form Date: 10/15/2020 9:38:25 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-6680765-046579
2a	Name:	Medication Assisted Treatment Study (MATS)
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: Business Steward POC Name: Bradley Biggers POC Organization: NCIPC POC Email: wmp0@cdc.gov POC Phone: 770.488.0562
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	December 24, 2020 ☐ Not Applicable

Save

11	Describe the purpose of the system.	The purpose of the system is to collect new information on the effectiveness of Medication Assisted Treatment Study (MATS)
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 type of information the system collects, maintain, and store are names, SSNs, email address, date of birth, phone numbers, medical notes, mailing address, education records, military status, employment status and demographic data such as gender, race, and ethnicity. All of the information collected to include SSNs are used to match vital statistics to determine whether participants have died. The project contains a secondary non-PII data analysis component consisting of analyzed health details from Physicians, that will compare electronic health record of three select data items, from data collected directly from providers. Users will be provided with a username and a one-time password that must be changed after the first login. All passwords created will follow the CDC password retention policy.
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The Medication Assisted Treatment Study (MATS) information system collect, maintain, and store name, SSNs, email address, date of birth, phone number, medical notes, mailing address, education record, military status, employment status and demographic data such as gender, race, and ethnicity. SSNs are collected from clients for use in locating clients that becomes lost to follow-up. All of the information collected to include SSNs are used to match vital statistics to determine whether participants have died. No credentials are collected, maintained stored, or shared. The project contains a non-PII secondary data analysis component that will compare electronic health record of three select data items to data collected directly from providers. (This is limited to 100 subjects at 2 sites, and data will be used exclusively to conduct a reliability assessment.) All the PII and non-PII data collections will be collected via commercially-available data collection software and stored on a secured server, then transferred to the third party contractor's secure systems. This information will not be shared or stored permanently. Prior to the end of the contract, all personal identifiable information will be destroyed prior to the system retiring.
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 ☒ 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 Gender Race/ethnicity User Name Passwords ☒ 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
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?	PII will be used to locate/contact clients and invite them to enroll in MATS.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	SSNs will be used to locate clients who are lost to follow-up. The study plans are to do follow-up interviews at 3, 6, 12 and 24 post-treatment initiation.
20	Describe the function of the SSN.	SSNs are collected from clients for use in locating clients that becomes lost to follow-up. The SSN will be used to match vital statistics to determine whether participants have died.
20a	Cite the **legal authority** to use the SSN.	E.O. 9397; E.O. 13478
21	Identify **legal authorities** governing information use and disclosure specific to the system and program.	Section 302 of the Public Health Service Act (42 U.S.C. 241) 280-1a; 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); E.O. 9397; E.O. 13478.
22	Are records on the system retrieved by one or more PII data elements?	○ Yes ◉ No

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.	The OMB information collection approval number is 0920-1218 and the expiration date is 2-28-2021.
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.	Clients will be notified in two ways that their PII will be collected. First, treating physicians will obtain explicit permission from clients to share their PII with the third party contractor's secure systems. Second, the third party contractor's project staff will administer a complete informed consent form to clients. The form explains to individuals the nature of the study, the data that will be collected from the individual (including PII) and the use of the data for the project. All participants will be made aware that the third party contractor will conduct public legal searches using their name and/or date of birth to track legal and criminal justice involvement. Participants will be made aware that Social Security Number may be used to track them should their participation in the study name.
26	Is the submission of PII by individuals voluntary or mandatory?	◉ Voluntary ○ Mandatory

Save

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.	Individuals can choose not to be referred to MATS. If they agree, they may refuse to participate in the study after reviewing the informed consent form. After agreeing to participate, at any point, individuals may refuse to answer any questions or participate further. Clients can also withdraw by contacting the the third party contractor's project director at anytime to withdraw from the study. Clients can request that their PII be removed from the third party contractor records and not be used for any subsequent purpose. Contact information for the third party contractor project director is provided in hard copy form to the client at the time of consent and in the study brochure provided by the referring physician.
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.	All clients give their permission prior to their participation in the evaluation data collection process. This permission process describes the process to notify individuals whose PII is in the system when major changes have occurred. We would then proceed to re-contact prior respondents using the same data collection information we last used to solicit their participation. In addition, at the next planned contact, clients not notified via previous contact information would be notified of any major system changes.
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.	Any issues experienced by research participants would be initiated by the participant in the study and resolved through the local 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.	The database administrator periodically reviews and compares the PII contained in the system against the spreadsheets/ database to ensure the data's integrity, availability, accuracy and relevance.
31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users: Users in the field will input data. ☒ Administrators: Administrative functions include creating user accounts, closing user accounts, and assigning roles to users. ☒ Developers: Developers maintain the application code and databases for the system. ☒ Contractors: Indirect contractors such as Field staff conducting interviews will be contracted through an approved third party contractor subcontractor. ☐ Others:
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Users roles are approved by the program management team and users cannot access PII without the appropriate roles, the program management team must approve all user role
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.	Role-based access control are in place to ensure the concept of "least privilege" is implemented. Job function determines the level of access and users are assigned only those rights necessary to fulfill responsibilities for approved roles. System-level audit controls to safeguard and audit use.

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.	All project staff are required to take annual training in cybersecurity, security awareness, privacy training, and Ethics training. This training has been reviewed and is compatible with CDC requirements and in accordance with contractual agreement.
35	Describe training system users receive (above and beyond general security and privacy awareness training).	All of the third party contractor's personnel on this project must complete Records Management Training and developers with administrative privileges completes IT Administrator Training.
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 (N1-442-09-1) and in accordance with contractual agreement. Record copy of study reports are maintained in agency 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 tapes, burning or shredding paper materials or transferring records to the Federal Records Center when no longer needed for evaluation and analysis. Records are retained for 20 years; for longer periods if further study is needed.
38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.	Administrative: Records are maintained according to specific CDC and RTI records control schedules and policy. PII is secured administratively by role-based access that limits information visibility only to those authorized to see it. Users will be required to have a username and password and will provide answers to periodic challenge questions. Project staff will be required to take training. Technical: The PII is secured using Level III two factor authentication as determined by the CDC Information Technology Services Office in the third party contractor's Moderate Network environment and secured server during transmission and form authentication with role-based access specific to the authenticated user. The data is encrypted at rest and in transmission. Project information is secured behind a firewall, on premise and will be transmitted in a secure manner. Physical: Servers are in an accessed-controlled server room, buildings secured by badge-accessed control, laptops are secured with end to end encryption, information is disposed of in accordance to contract requirements.

General Comments	Q10: This system has changed business steward and no longer use social security numbers.

Save

OPDIV Senior Official for Privacy Signature	Jarell Oshodi -S Digitally signed by Jarell Oshodi -S Date: 2020.12.07 09:18:21 -05'00'