Save

Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-33127 | Form Date: 8/6/2019 2:03:22 PM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-4081881-815547
2a	Name:	STEADI Older Adult Hospital Discharge Opioid Prescribing (OAHDOP)
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.	Implementation
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: Behavioral Scientist POC Name: Gwendolyn Bergen POC Organization: CDC/ONDIEH/NCIPC/DUIP POC Email: gjb8@cdc.gov POC Phone: 770.488.1394
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	November 5, 2019 ☐ Not Applicable

Save

11	Describe the purpose of the system.	The purpose of the system is to collect information to determine the impact of performing medication management for opioids as part of hospital discharge on older adult re-admissions and falls and injuries related to falls.
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 information system will collect, maintain and store patient's name, email address, phone number, medical notes, date of birth, and mailing address. Other data includes clinical data, patient reports and data from primary care physicians. Users for this system are authenticated via Active Directory (AD) and User Ids and passwords are stored in the system. AD is a separate system with its own PIA.
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	STEADI Older Adult Hospital Discharge Opioid Prescribing (OAHDOP) is a full moderate information system that Evaluate the ability to influence opioid prescribing patterns and use among older adults following discharge from an inpatient setting. Clinical work-flow data collected will be stored and managed within the UCSF electronic medical record as standard parts of the UCSF Epic EHR. Data collected will take the form of flow sheets, standard reports used to manage clinical work, and data extracts contained in epic standard data tables (e.g. Clarity data warehouses). The information system will collect, maintain and store patient's name, email address, phone number, medical notes, date of birth, and mailing address. Other data includes clinical data, patient reports and data from primary care physicians. Patient reported data will be collected directly from patients via in-person interviews, phone and electronic mail surveys sent at regular intervals after discharge from the hospital. This data will be collected under existing approvals by the UCSF Institutional Review Board (the UCSF body charged with ensuring data security and privacy, as well as patient safety and protections under research protocols). Data from these activities will be housed in UCSF's highly secure data infrastructure (details of which can be found at: https://myresearch.ucsf.edu/myresearch). Data collected from patients will be stored temporarily. Data from Primary Care Physicians will be collected via direct contact with a small sample of physicians, either from faxed surveys, emailed surveys, or phone calls. Clinical data, medical and patient reports from these activities will be housed in the same infrastructure as patient data stated above. The data will be stored temporarily until the contract ends. This information will be shared only with the CDC. Users for this system are authenticated via Active Directory (AD) and User credentials, Ids and passwords are stored in the system. AD is a separate system with its own 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 User credentials (Ids and passwords)
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: Clinical Providers
17	How many individuals' PII is in the system?	500-4,999
18	For what primary purpose is the PII used?	The PII is used primarily for contact and follow-up.
19	Describe the secondary uses for which the PII will be used (e.g. testing, training or research)	N/A
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).
22	Are records on the system retrieved by one or more PII data elements?	◉ Yes ○ No

Save

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:	09-20-0136, Epidemiologic Studies and Surveillance of Disease Problems
		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.	The OMB information collection approval number and expiration date is pending.	
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.	During the initial process, potential participants are contacted and notified of what will be collected, and written consent will be obtained. If they object they cannot fill out the survey. Also during the survey the participant can change his/her mind and elect not to complete the survey.	
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.	Individuals can opt-out by simply choosing not to participate in the survey. In addition, individuals will be advised that they can at any time opt-out of the study or refuse to answer any questions they do not wish to answer.	

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.	The process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system will be notified by email or regular mail when there are any major changes to the 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.	Individuals with concerns about PII, inappropriate attainment, use or disclosure as well as inaccuracy of their PII may report their concerns to the STEADI OAHDOP Information System Security Officer (ISSO) or the Contracting Officer's Representative (COR) for the contract. They may also report the incident to the Project Director for the contract that supports the task. The Project Director point of contact and phone number is Jeffrey Toole at 703-801-0144.
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/web administrator periodically reviews and compares the PII contained in the system against the spreadsheets/database to ensure the data's integrity, availability, accuracy and relevancy.
31	Identify who will have access to the PII in the system and the reason why they require access.	☒ Users: To conduct interviews or manage the data collection process. ☒ Administrators: Administrators have full rights to maintain and support the overall system. ☐ Developers: ☒ Contractors: In-direct contractors need access to manage the data collection process. ☐ Others:
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Contractor uses the concept of Role-Based Access Control (RBAC) to give the appropriate permissions associated with each role. RBAC uses the security principle of least privilege to
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 will be used to allow those with access to PII to be able to access the minimum amount of PII needed to perform their job. Users must request access to specific files needed and that is the only access they are permitted. No one is granted more access than is 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.	All personnel having system access are required to take the Privacy and IT Security Awareness training upon hire and annually thereafter. This training has been reviewed and is compatible with CDC requirements to make them aware of their responsibilities for protecting the information being collected and maintained.
35	Describe training system users receive (above and beyond general security and privacy awareness training).	All system users are required to complete annual training requirements that consist of HIPAA, and Ethics and Compliance.

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.	Records are retained and disposed of in accordance with the CDC Records Control Schedule (NI-442-09-1 and in accordance with contractual agreement. Record copy of study reports are maintained in the agency from two to three years in accordance with retention schedules. Source documents for the 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.	PII will be secured using the following: Administrative controls include a system security plan, contingency plan, regular back-up files and storage of backups off-site, role-base security awareness training, least privilege access (enforced through Active directory groups), separate user and privileged accounts for administrators, policies and procedures for retention and destruction of PII and a corporate incident response team and incident response plan. Technical controls include identification and authentication using unique user IDs, passwords, and smart cards, use of firewalls and intrusion detection and prevention systems, virus scanning software on all computers and a security information and event management solution. Physical controls include guards, identification badges, key cards and closed circuit TV.
	General Comments	
	OPDIV Senior Official for Privacy Signature	Jarell Oshodi -S Digitally signed by Jarell Oshodi -S Date: 2019.08.07 15:17:58 -04'00'