Save

Privacy Impact Assessment Form

v 1.47.4

Status: Draft | Form Number: F-94855 | Form Date: 3/22/2017 8:15:30 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-1493325-640424
2a	Name:	Test Predictability of Falls Screening Tool (TPFST)
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.	Design
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	April 20, 2017 ☐ Not Applicable

Save

11	Describe the purpose of the system.	The Test Predictability of Falls Screening Tool (TPFST) is being designed as a data repository and management system for the fall risk screening initiative by CDC/National Center for Injury Prevention and Control (NCIPC). As such, it will store responses to the screening questions asked of the study participants s well as enable the project staff to track the progression of cases during the project. TPFST will facilitate clinicians' ability to identify adults 65 and older who are likely to fall and thus will need additional, specialized care in the future. Although there are a number of tools used to screen older adults for fall risk, there is currently no standard for fall risk screening across care settings. It is anticipated that the questions asked and the results identified via this tool will be recommended for use by CDC as the standard for screening of falls for adults 65 and older in clinical settings. Questions will be asked to a nationally representative sample of adults 65 and older, who will then be followed with surveys repeated monthly over the following year to determine whether and how often they fall.
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 TPFST will collect and store case-level call history data to track the status of a screened case, and study participants' responses to the screening questions. The screening questions will determine patients' risk levels for falls.
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	TPFST will collect and store the information obtained as part of this study, to include both case-level call history data and participant responses to questionnaires. The call history data will be stored in the system separately from the questionnaire data. Questionnaire data will include participant/respondent contact information, demographics, access to preventive health, falls screening questions, and health outcomes. All data stored in TPFST will be maintained by the contractor, NORC, on behalf of CDC. As part of the data collection process, respondents will be contacted via mail or telephone. Mailed letters will contain the web link for the online survey, the respondent's unique PIN, and instructions on how to access the survey. Also, respondents will have the option of calling the study's toll-free line at any time to complete the survey via telephone with a trained data collection specialist. Response data from the questionnaires will be used for analysis purposes and to prepare reports, reporting information in the aggregate. De-identified data files will be delivered to the CDC twice throughout the survey; once at the midpoint and at the end. A final, cleaned dataset will be delivered at the end of the project.
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 ☒ 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?	500-4,999
18	For what primary purpose is the PII used?	PII will be used to contact participants, both initially and for 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.	TBD	
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.	The contractor, NORC, uses a probability based panel designed to be representative of the US population to produce a nationally representative sample. Participant panels are recruited from this sample. During this recruitment process, potential participants are contacted, notified what is being collected and given the opportunity to self-select the surveys of interest to them. They are later contacted for the actual survey, and during the scripted introduction and screening, they are again given notice and can consent or object to actual participation in the survey. Names and addresses are not delivered to CDC.	

Save

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 of the study. During the introductory script 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.
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.	Electronic or regular mail is sent 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 inappropriate attainment, use, or disclosure as well as inaccuracy of their PII may report their concerns to the TPFST Information Systems Security Officer (ISSO) or the Contracting Officer's Representative (COR) for the contract that supports TPFST. They may also report the incident to the Project Director for the contract that supports TPFST and/or the TPFST Helpdesk where their concern must be logged and submitted to CDC.
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.	Data collection will occur monthly over one year. Respondents will be asked to confirm/update their contact information for recontact in the future. Respondents can also contact the project via a toll-free telephone number or project e-mail address to alert the project staff to any changes in contact information (name, address, phone). These methods will serve as the primary manner in which the data is reviewed for 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 and support the overall system. ☐ Developers ☐ Contractors ☐ Others
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Role Based Access Control (RBAC) will be used to determine who has 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.	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.

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 NORC (contractor) employees are required to take Privacy and IT Security Awareness training annually. This training has been reviewed and is compatible with CDC requirements.
35	Describe training system users receive (above and beyond general security and privacy awareness training).	All NORC (contractor) staff are required to undergo annual Ethics and Compliance training which has been reviewed and is compatible with CDC requirements. The project staff will receive system specific training prior to system use. All project staff will be required to sign the information system Rules of Behavior document and a non-disclosure agreement.
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 controls include a system security plan, contingency plan, regular back up of files and storage of backups off site, role-based security awareness training, least privilege access enforced through Active Directory groups, separate user and privileged accounts for administrators, policies and procedures in place for retention and destruction of PII, and a corporate incident response team and incident response plans. Technical controls include identification and authentication using unique user IDs, passwords, and smart cards, use of firewalls and intrusion detection/prevention systems, virus scanning software on all computers, and a security information and event management (SIEM) solution. Physical controls include guards, identification badges, key cards, and closed circuit TV.
General Comments		

Save

OPDIV Senior Official for Privacy Signature	Beverly E. Walker -S	Digitally signed by Beverly E. Walker -S Date: 2017.09.15 18:21:53 -04'00'