Save

Privacy Impact Assessment Form

v 1.47.4

Status Draft Form Number F-80142 Form Date 8/5/2019 7:36:50 AM

	Question	Answer
1	OPDIV:	CDC
2	PIA Unique Identifier:	P-1496061-751658
2a	Name:	STEADI Cost Effectiveness (SCE)
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 4, 2019 □ Not Applicable

Save

11	Describe the purpose of the system.	The purpose of this project is to implement the CDC’s STEADI (Stopping Elderly Accidents, Deaths, and Injuries) initiative into outpatient practice in a health system, evaluate the impact on falls and medically treated falls, and develop a cost effectiveness for the STEADI initiative. A full implementation of STEADI will be tested along with two modified implementations. Data will be collected from providers, research nurses, clinical nurses, IT staff, practice managers, and patients to improve the implementation.
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, mailing address and user credentials (Userid and password). The Pin is not collected or stored. Data will be collected from providers to improve the implementation and from patients to obtain their falls record and understand their fall prevention behaviors. Other data collected include identifying patients risk of falling; assessments to identify which fall risk factors are present. (e.g., medication review, functional ability test, visual acuity, orthostatic blood pressure, podiatry review, vitamin D intake, and home hazard evaluation), strategies to reduce fall risk. (e.g., strength and balance program, manage medications, occupational therapy, vitamin D supplements, corrective eyewear). A full implementation of STEADI will be tested along with two modified implementations. Data will be collected from providers to improve the implementation and from patients to obtain their falls record and understand their fall prevention behaviors. This will include STEADI implementation and process questions, practice cost of implementation questions and feedback from patients. Data will also be collected from providers, research nurses, clinical nurses, IT staff, practice managers, and patients to improve the implementation. Interviews will be conducted with providers, research nurses, clinical nurses, IT staff, practice managers, and patients. Data will be collected in-person using hard-copy questionnaires. All data collected will be stored temporarily or until contract expires.

Save

13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	STEADI Cost Effectiveness (SCE) is a full Moderate information system whose purpose is to implement the CDC's STEADI (Stopping Elderly Accidents, Deaths, and Injuries) initiative into outpatient practice in a health system, evaluate the impact on falls and medically treated falls, and develop a cost effectiveness for the STEADI initiative). STEADI is a suite of materials intended to help healthcare providers implement the clinical practice guidelines developed by the American and British Geriatric Societies for prevention of falls among older Americans. STEADI includes the following core elements such as screening to identify patients at increased risk of falling; assessments to identify which modifiable fall risk factors are present. (e.g., medication review, functional ability test, visual acuity, orthostatic blood pressure, podiatry review, vitamin D intake, and home hazard evaluation), and intervene using effective strategies to reduce fall risk. (e.g., strength and balance program, manage medications, occupational therapy, vitamin D supplements, corrective eyewear). A full implementation of STEADI will be tested along with two modified implementations. Data will be collected from providers to improve the implementation and from patients to obtain their falls record and understand their fall prevention behaviors. This will include STEADI implementation and process questions, practice cost of implementation questions and feedback from patients. The information system will also collect, maintain and store patient's name, email address, phone number, mailing address and user credentials (Userid and password). The Pin is not collected or stored. Data will be collected from providers to improve the implementation and from patients to obtain their falls record and understand their fall prevention behaviors. Data will also be collected from providers, research nurses, clinical nurses, IT staff, practice managers, and patients to improve the implementation. Interviews will be conducted with providers, research nurses, clinical nurses, IT staff, practice managers, and patients. Data will be collected in-person using hardcopy questionnaires. All data collected will be stored temporarily or until contract expires.
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 user id and password
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

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.	The participants are informed that personal information would be collected prior to consent to do interview. At the time of screening all participants, interviewers will include information about how the data will be used.
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.	The participants can decline to participate in the study altogether or withdraw their participation at anytime. If they want to opt-out prior to or after completing the survey, they can do so by contacting the IT Security Compliance Manager at (312) 759-2667.
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.	Study personnel will contact participants via email and phone number on record to notify and obtain consent when major changes occur 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.	The participants may report their concerns about any erroneous PII or any inappropriate attainment, use or disclosure to InformationSecurity@norc.org or call 888-879-6672.

Save

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.	NORC admin periodically (every quarter) reviews and compares the PII contained in the system for the participants against the 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	NORC users conduct interviews and or manage the data collection process.
		☒ Administrators	NORC Admins 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.	The Contractors, Administrators and developers may be granted access to the data. Access is based on role-based Access control and the least privilege method as authorized by	
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. All access is granted through Active Directory. Individual Active Directory groups are created for each project. Only the project staff that require access are added to the project group.	
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 staff are required to take annual training in cybersecurity, security awareness and privacy training. 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 system users are required to receive annual system specific training on system use, Health Insurance Portability and Accountability Act (HIPAA), Ethics, and Compliance.	
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 retention is 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.	

Save

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. During the study, data is secured through the use of technical, physical, and administrative controls. All data is stored in a secure data center with limited access. All access is via electronic card readers. The data center has special environment controls to monitor for disruption to electrical or air conditioner failure. 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. Servers and workstations are protected with anti-virus software. Their configuration follow the Computer Internet Security configuration and FDCC standard. Security patches are automated and applied at least monthly depending on the criticality of the patch. All systems have vulnerability scans performed monthly. Physical controls include guards, identification badges, key cards, and closed circuit TV.Data backups are encrypted and sent off site in case of disaster at the primary processing facility.

General Comments	Q40a: In accordance with HHS's "Rescission of Office of the Chief Information Officer/Superseded Policy for Machine Readable Privacy Policies and Related Guidance Documents" memo. MRPP cannot be validated due to obsolete technology and the suspension of work on P3P by the Platform for Privacy Preferences Project workgroup.
OPDIV Senior Official for Privacy Signature	Jarell Oshodi -S Digitally signed by Jarell Oshodi -S Date: 2019.09.12 10:57:17 -04'00'