Privacy Impact Assessment

For The

Registry of Patient Registries (RoPR)

The Agency for Healthcare Research Quality
US Department of Health and Human Services
5600 Fishers Lane
Rockville, MD 20857

January 31, 2017

PIATemplate last updated June 25, 2014

Instructions: See HHS Information Technology Security Program PIA Guide v1.0, 2013-07-03

If answer to #14 is no, disregard questions #15-33.

Item	Question	Response
1	OPDIV	AHRQ
2	PIA Unique Identifier	P-9496384-979384
2a	Name	Registry of Patient Registries
3	The subject of this PIA is which of the following? (Select one.)	Minor Application (stand-alone)
3a	Identify the Enterprise Performance Lifecycle Phase of the system.	Operations and Maintenance
3b	Is this a FISMA-Reportable system?	Yes
4	Does the system include a website or online application available to and for the use of the general public?	Yes
5	Identify the operator.	Contractor
6	POC	1. Title: IT Project Manager 2. Name: Woody Walker 3. Organization: Truven Health Analytics 4. Email: Woody.Walker@truvenhealth.com 5. Phone: (805) 979-3726
7	Is this a new or existing system?	Existing
8	Does the system have Security Authorization (SA)?	Yes
8a	Date of security authorization.	7/15/2016
8b	Planned date of security authorization.	4/1/2017
9	Indicate the following reason(s) for updating this PIA. Choose from the following options.	☐PIA Validation (PIA Refresh/Annual Review) ☐ Anonymous to Non-anonymous ☒ New Public Access ☐ Internal Flow or Collection ☐ Commercial Sources ☐ Significant System Management Change

		☐ Alteration in Character of Data ☐ New Interagency Uses ☐ Conversion ☐ Other: [*Please specify*]
10	Describe in further detail any changes to the system that have occurred since the last PIA.	System will facilitate direct updates to content of Website by members of the public. To facilitate this functionality, a self-registration and authentication feature will be developed and incorporated into the application. The authentication feature will require users to provide PII.
11	Describe the purpose of the system.	The Registry of Patient Registries (RoPR) is a database system designed to meet the following objectives: 1) Provide a searchable database of existing patient registries in the United States; 2) Facilitate the use of common data fields and definitions in the similar health conditions to improve opportunities for sharing, comparing, and linkage; 3) Provide a public repository of searchable summary results, including results from registries that have not yet been published in the peer-reviewed literature; 4) Offer a search tool to locate existing data that researchers can request for use in new studies; and 5) Connect patient registries with individuals interested in learning more about them and how they advance healthcare. 6) Serve as a recruitment tool for researchers and patients interested in participating in patient registries.
12	Describe the types of information the system will collect, maintain (store), or share.	The RoPR collects metadata on patient registries, which is voluntarily submitted to promote collaboration, reduce redundancy, and improve transparency in registry research. Info collected include: - Registry title (Official) - Version - Registry description (long & short) - Geography and location - Registry classification - Registry purpose - Interested in being contacted - Organization - Contact (first & last name) - Contact email - Contact phone - Reasons for contact - Condition of access - Link to registry or organization Web site - Has Data Monitoring - Progress report

		- Title - Summary - Number of Participants - Length of Follow-up - Report URL - Related information - Condition/service focus of registry - Category of interest for registry - Type of ID - ID Number - Start Date Month - Start Date year - Enrollment Type - Primary Completion Date Month (if applicable) - Primary Completion Date Year (if applicable) - Primary Completion Date Type (drop down) - Completion Date Month (if applicable) - Completion Date Year (if applicable) - Completion Date Type (if applicable) - Recruitment Status - Collaborators (Name) - Observational Study Model - Time Perspective - Biospecimen Retention - Enrollment: Number of Subjects - Enrollment: Type - Target Follow-Up Duration - Target Follow-Up Duration (drop down) - Group/Cohort Label - Group/Cohort Description - Intervention Type - Intervention Name - Intervention Other Names - Intervention Description - Primary Outcome Measure Title - Primary Outcome Measure Time Frame - Primary Outcome Measure Description - Primary Outcome Measure Safety Issue - Secondary Outcome Measure Title - Secondary Outcome Measure Time Frame - Secondary Outcome Measure Description - Secondary Outcome Measure Safety Issue - Other Outcome Measure Title - Other Outcome Measure Time Frame - Other Outcome Measure Description - Other Outcome Measure Safety Issue - Sampling Method

		- Study Population Description - Eligibility Criteria - Gender - Minimum Age - Minimum Age (drop down) - Maximum Age - Maximum Age (drop down) - Accepts Healthy Volunteers - Publications (PubMed ID or Citation) - Accepts Electronic Public Health Data - Providers Served - Public Health information Administrative mandatory and optional information which is not disseminated or made public contains PII. - Mandatory administrative PII: - Username - Password - E-mail - Optional administrative PII - First name - Last name - Organization The RoPR is accessible to the public via the internet. It supports browser-based internet access and is located at patientregistry.ahrq.gov. Users browsing/searching registry information on the RoPR do not require user authentication. The primary users of the system are members of the public who are interested in patient registries. This includes: funding agencies; government, regulatory, and public health agencies; pharmaceutical and device manufacturers; biomedical journal editors; patients and healthcare consumers; healthcare payers; healthcare providers; healthcare professional associations; and researchers.
13	Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.	The RoPR is a custom system environment. The application is accessible to users as a Web site, which can be accessed via the internet in a Web browser. The application is accessible to the public via a web server and users can conduct keyword searches to find relevant patient registries. This portion of the application is read-only and does not collect any information from public users. The registry information that is publicly searchable is entered directly into the system by the registry owners themselves. This

		publicly accessible information could contain PII, but entry of PII for display is strictly optional by the registry owner. The sub-section of the RoPR, called the Registry Registration System (RRS), is where users can enter data into the system. It is accessible via a secure session authentication. Before a new registry can be entered into RoPR, new record owners must create a username and password. An email address is also mandatory to facilitate communication between AHRQ and the record owner. The record owner may also choose to provide their name and organization but providing that additional information is strictly optional. This information associated with the record owner is not made public. The optional information will only be used to help validate the veracity of the registry and the registry owner information. The mandatory information is used to facilitate authentication for the record owner to update their own registry information. The email will only be used for periodic auto-generation of e-mail reminders pertaining to the maintenance of RoPR patient registry data and resetting of passwords. There is no human administrator that is pulling this information for the purpose of sending out e-mails. All of the information described above will be kept permanently unless requested by the registry owner to be removed. Users may also authenticate through the Protocol registration and Results System (PRS) at https://register.clinicaltrials.gov/ in order to access the RoPR data entry system, RRS. The RoPR team has worked with the ClinicalTrials.gov team, at the National Library of Medicine, to ensure session connections are properly restricted. Once the user is authenticated at PRS, there is no additional username and password authentication required to access RRS. The secure connection is maintained between the ClinicalTrials.gov white-listed IP addresses and the RoPR system.
14	Does the system collect, maintain, use or share PII?	Yes
15	Indicate the type(s) 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 ☒ URL(s) ☒ Other: [*Please specify*]
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: [*Please specify*] Patient registrars; corporations and research organizations who are not business partners/contacts/vendors/suppliers/or contractors of the RoPR
17	How many individuals' PII is in the system?	Currently there are 2668 patient registries on the RoPR system. This count is periodically updated as new registries are listed in the system. Only the PII of the RoPR self-designated contact responsible for maintaining the registry's data is in the system.
18	For what purpose is the PII used?	The RoPR collects metadata on patient registries which is voluntarily submitted to promote collaboration, reduce redundancy, and improve transparency in registry research. Administrative information which contains PII about the registry record owner is required to provide authentication and authorization of the record owner identification to facilitate their updating of the registry information. The registry information, which is publicly available, consists of contact information pertaining to outreach from the general public or additional information related to the patient registry record. Administrative information is used by the agency for contacting

		users (i.e. record owners) regarding the maintenance of their records. Publicly available information allows the general public to contact the record holder for additional information about the patient registry. Both Administrative and publicly available information contains PII. Some of the administrative information is mandatory if the record owner wants to add a registry, whereas publicly available information is voluntary.
19	Describe the secondary uses for which the PII will be used (e.g., testing, training, research)	There are no secondary uses for which the PII will be used.
20	Describe the function of the SSN	Not applicable.
20a	Cite the legal authority to use the SSN	Not applicable.
21	Cite the legal authorities governing information use and disclosure specific to the system and program.	5 U.S.C. 301, Departmental regulations, Section 944(c) of the Public Health Service Act (42 U.S.C. 299c-3(c)) ("the AHRQ Confidentiality Statute"), E-Government Act of 2002; OMB M-03-22, OMB 07-16, OMB M-10-23.
22	Are records on the system retrieved by one or more PII data elements?	No
22a	Identify the number and title of the Privacy Act System of Records Notice(s) being use to cover the system or identify if a SORN is being developed.	Not applicable
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 [*Please specify*] Government Sources: ☐ Within the OPDIV ☐ Other HHS OPDIV ☐ State/Local/Tribal

		☐ Foreign ☐ Other Federal Entities ☐ Other [*Please specify*] Non-Government Sources: ☐ Members of the Public ☐ Commercial Data Broker ☐ Public Media/Internet ☒ Private Sector ☐ Other [*Please specify*]
23a	Identify the OMB information collection approval number and expiration date.	#0935-0203, renewed on March 11, 2016. Expiration is March 31, 2019
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 [*see below*] ☒ Other Federal Agency/Agencies [*see below*] ☒ State or Local Agency/Agencies [*see below*] ☒ Private Sector [*see below*] ☒ Other [*see below*] Publicly available PII in the patient registry listing on RoPR is disclosed to allow the general public to contact the record holder for additional information about the patient registry.
24b	Describe any agreements in place that authorize the information sharing or disclosure (e.g., computer matching agreement, information sharing agreement, or memorandum of understanding).	The primary purpose of RoPR is to share and disseminate information about patient registries. Participation in RoPR is strictly voluntary and registry owners are not required to provide PII for public disclosure, only if they wish to be contacted. Before completing their registration on the system, registry owners will have to acknowledge a click wrap agreement agreeing to having their PII disclosed if they have entered contact information. "By selecting 'I Agree' below, I give my consent to having my contact information, where completed as part of the registry listing, made publicly available to anyone who visits the RoPR Web site."
24c	Describe the procedures for accounting for disclosures	Not applicable.
25	Describe the process in place to notify individuals that their personal information will be	Before completing their registration on the system, registry owners will have to acknowledge a click wrap agreement agreeing to having their PII disclosed if they have entered

	collected. If no prior notice is given, provide a reason.	contact information. "By selecting 'I Agree' below, I give my consent to having my contact information, where completed as part of the registry listing, made publicly available to anyone who visits the RoPR Web site."
26	Is the submission of PII by individuals voluntary or mandatory?	Voluntary for PII for public disclosure. Mandatory for PII used for administering the patient registry record owner account (PII not shared or disclosed).
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.	Registering a patient registry on RoPR is strictly voluntary, so the registry owner is choosing to opt-in to the collection of their PII, therefore an opt-out option is not necessary. Once the registry owner has opted to create an account on RoPR, there is no opt-out for the registry owner's e-mail address which is required for the administration of the registry owner's system account to maintain their RoPR patient registry listing.
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.	(1) Major changes to the system would be subject to AHRQ and stakeholder review. Any plans for notification and consent would be determined as part of a change control process if appropriate. (2) The change control process will include the specifics regarding collection of PII. (3) Any changes related to notification and consent regarding PII will be reflected on-screen and in help text available within the system. (4) Registry record owners will be contacted using the email address on record to notify them of changes to how their PII will be utilized. The registry holder is responsible for ensuring their information is correct and up to date. Annual reminders are sent to registry holders to keep their account current.
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, provide a reason.	Contact information for the RoPR system is available on the Web site. FAQ section also has instructions for users on how to resolve issues related to PII. The registry holder may contact the RoPR support team with any concerns. They may also update their contact information as necessary.
30	Describe the process in place for periodic reviews of PII contained in the system to ensure that the data's integrity, availability, accuracy and relevancy. If no processes are	Data checks by the registry holder are completed before information is posted. The user confirms via checkbox that all information is accurate to the best of their knowledge; and is responsible for ensuring continued accuracy after submission.

	in place, provide a reason.	Annual reminders are sent to registry holders to keep their account current.
31	Identify who will have access to the PII in the system and provide a reason why they require access.	General public will have access to the PII (contact information) entered for public display by the record owners along with the patient registry listing in RoPR. However, the mandatory PII about the record owner required as administrative information for the registry listing and account registration will only be accessible to: ☐ Users: [*Please specify*] ☒ Administrators: system administration and support ☒ Developers: system update and troubleshooting ☒ Contractors: play administrator or developer role ☐ Others: [*Please specify*]
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Administrators have privileged access to the system and ultimately all information stored on the system itself. Administrators perform activities like adding and removing user accounts, promoting system changes, and backup-recovery tasks. Developers also have privileged access to the system to test/checkout changes and troubleshoot issues. Since PII is an integral part of the functionality of the RoPR system, the developer needs access to the database containing PII to test functionality or troubleshoot. Contractors may be in an administrator or developer role with the same privileges to access.
33	Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to do their jobs.	Access to the computing facility is restricted to specifically identified personnel and contractors with a legitimate business need for access. Access to servers is restricted to specified personnel and contractors. Logon to the servers is only possible after authentication; all non-secure modes of access are disabled. Access to the application is restricted to those individuals granted access through an account and password. All personnel with access to the system have been trained in the protection of PII, with records of that training maintained. PII is stored in a MySQL database. Direct access to the database will be blocked by the firewall and server authentication. Internally, the MySQL instance will only accept connections from a limited set of IP addresses. In addition, need-to-know

		access will be enforced by username/password.
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 of the listed training and materials are completed and reviewed annually: - HIPAA Privacy & Security Training for all employees and contractors - AHRQ Information Systems Security Awareness Training for all employees and contractors - HHS Information Security for IT Administrators - HHS Rules of Behavior for all employees and contractors - HHS Rules of Behavior Addendum for Privileged Users
35	Describe the training system users receive above and beyond the general security and privacy awareness training.	Depending on the staff member's specific role or responsibilities, individuals will receive specific training as required to fulfill their duties such as the "HHS Information Security for IT Administrators".
36	Do contracts include Federal Acquisition Regulation (FAR) and other clauses ensuring adherence to privacy provisions and practices?	Yes
37	Describe the process and guidelines in place with regard to the retention and destruction of PII. Cite specific records retention schedules.	The PII collected is stored in a secure database, backups are encrypted and stored. The backups are maintained as long as required by legal and regulatory requirements, and subsequently AHRQ is consulted to determine whether the PII should be destroyed. Destruction of records is scheduled for 20 years after completion of signed agreements per National Archives and Records Administration, Disposition Authority Number DAA-0510-2013-0003-0001.
38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical and physical controls.	Administrative controls - Annual security and privacy training - Manager approval to grant system access - Detailed tracking of user access accounts - Quarterly access control review - Separation of duties - Least privilege - Continuous monitoring - Security assessments and authorization of system Technical controls - User identification - Passwords with rules enforced (complexity, expiration, history)

		- Encryption during sessions (SSL, SSH) - Detailed logging of user account activities - Monthly vulnerability scans - Network monitoring (IDS/IPS) - Network segmentation / firewalls Physical controls - Restricted access - key cards and biometrics - Video camera surveillance - Emergency power – UPS and backup generators for power - Inventory and tracking of information system components
39	Identify the publicly-available URL(s).	https://patientregistry.ahrq.gov
40	Does the website have a posted privacy notice?	Yes
40a	Is the privacy policy available in a machine-readable format?	Yes
41	Does the website use web measurement and customization technology?	Yes
41a	Select the type of website measurement and customization technologies in use, and if they are used to collect PII. (Select all that apply).	Technology: / Collects PII? ☐ Web Beacons / ☐ Yes ☐ No ☐ Web Bugs / ☐ Yes ☐ No ☒ Session Cookies / ☐ Yes ☒ No ☐ Persistent Cookies / ☐ Yes ☐ No ☐ Others: [*Please specify*] / ☐ Yes ☐ No
42	Does the website have any information or pages directed at children under the age of thirteen?	No
43	Does the website contain links to non-federal government websites external to HHS?	Yes
43a	Is a disclaimer notice provided to users that follow links to websites not owned or operated by HHS?	Yes. Next to each link, it states: "By clicking on this link, you are leaving this Federal Government Web site and re-directed to a non-Federal Web site."