Privacy Impact Assessment

For The

Registry of Patient Registries (RoPR)

The Agency for Healthcare Research Quality
US Department of Health and Human Services
540 Gaither Road
Rockville, MD 20850

January 15, 2016

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: Nelly Mentor 3. Organization: Quintiles Real World Late Phase Research 4. Email: Nelly.Mentor@Quintiles.com 5. Phone: (617) 475-6489
7	Is this a new or existing system?	Existing
8	Does the system have Security Authorization (SA)?	Yes
8a	Date of security authorization.	11/1/2012
8b	Planned date of security authorization.	-
9	Indicate the following reason(s) for updating this PIA. Choose from the following options.	PIA Validation (PIA Refresh/ Annual Review)
10	Describe in further detail any changes to the system that have occurred since the last PIA.	N/A
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) 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.	1) 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 is not disseminated, consists of an e-mail address. 2) Administrative information will be used exclusively by the agency for contacting users 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. 3) Both Administrative and publicly available information contains PII. Administrative information is exclusively an e-mail address. Publicly available information contains name, e-mail address, and/or web URLs. 4) Administrative information is mandatory. Publicly available information is voluntary. The RoPR is accessible to the public via the internet. It supports browser-based internet access and is located at www.patient-registries.ahrq.gov. Users browsing material 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. The sub-section of the RoPR, called the Registry Registration System (RRS) where users can enter data into the system, is accessible via a secure session authentication. Users must navigate to it through www.ClinicalTrials.gov in order to access the data entry system, and the RoPR team has worked with the ClinicalTrials.gov team at the National Library of Medicine to ensure session connections are properly restricted. There is no username or password connected, and the users' identity is not verified upon entry to RRS. The 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.	• Name • E-mail Address • Phone Numbers • Web URL
16	Indicate the categories of individuals about whom PII is collected, maintained, or shared.	• Public Citizens • Other: 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 140 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?	1) The RoPR collects metadata on patient registries which is voluntarily submitted to promote

		collaboration, reduce redundancy, and improve transparency in registry research. Administrative information, consists of a contact e-mail address and phone number. 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. (2) Administrative information is used by the agency for contacting users 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. (3) Both Administrative and publicly available information contains PII. Administrative information is an e-mail address. Publicly available information contains name, e-mail address, and/or registry website URLs. (4) Administrative information is mandatory, 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	SSN is not requested, collected or maintained
20a	Cite the legal authority to use the SSN	SSN is not requested, collected or maintained
21	Cite the legal authorities governing information use and disclosure specific to the system and program.	Section 913 and 306 of the Public Health Service (PHS) Act (42 U.S.C. § 299b-2 and 242k(b)). Sections 924(c) and 308(d) of the PHS Act (42 U.S.C. 299c-3(c) and 242m(d)) provide authority for protecting restrictions on identifiable information about individuals. Privacy Act of 1974; 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.	SORN is not required as there are no RoPR records under the control of AHRQ from which information can be retrieved by the name of the individual or by some identifying number, symbol, or other identifier assigned to the individual.
23	Identify the sources of PII in the system.	Directly from an individual about whom the information pertains: Online Non-Government Sources: Private Sector
23a	Identify the OMB information	#0935-0203, expired on October 31, 2015.

	collection approval number and expiration date.	A new OMB information collection approval number and expiration date is pending, late January 2016.
24	Is the PII shared with other organizations?	Yes
24a	Identify with whom the PII is shared or disclosed and for what purpose.	• Within HHS • Other Federal Agency/Agencies • State or Local Agency/Agencies • Private Sector Publicly available PII 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).	Memorandum of Understanding (MOU), Interconnection Security Agreement (ISA)
24c	Describe the procedures for accounting for disclosures	There is a complaint process in place for individuals who believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. Contact information for the RoPR system is posted where the PII is shared.
25	Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, provide a reason.	In the RoPR registration interface, there is a disclaimer clearly stating: "This email will only be used by RoPR and will not be distributed."
26	Is the submission of PII by individuals voluntary or mandatory?	Voluntary
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.	There is no opt-out for the registry contact's name and e-mail address is required for the periodic generation of e-mails pertaining to the maintenance of RoPR patient registry data.
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,	(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

	describe why they cannot be notified or have their consent obtained.	regarding PII will be reflected on-screen and in help text available within the system. 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, otherwise the account is archived following 4 years of inactivity.
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 posted where the PII will be shared. 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 in place, provide a reason.	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.
31	Identify who will have access to the PII in the system and provide a reason why they require access.	• Users – any PII entered is publicly accessible. • Administrators – any PII entered is publicly accessible. • Developers – any PII entered is publicly accessible.
32	Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.	Quintiles Corporate Policy QCP_RB_CDP0005: "Rules Based Corporate Policy – Protection of Personal Information" sets forth Quintiles' commitment to protect personal information from unauthorized use, disclosure, access, or loss that can result in substantial harm to individuals, including identify theft or other fraudulent use of such information. This Corporate Policy applies globally to all directors, officers, employees (including contractors and temporary staff), and agents of Quintiles (or the "Company").
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 systems is by encrypted

		key-based 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 will be blocked by the firewall. 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.	• HIPAA Privacy & Security for US IT & HR New Employees • Quintiles' Learning Curve Online Course, G004182: Global Safety and Security intends to help staff understand the framework for our environmental, health, safety and security programs. This course is assigned to all active employees, including new hires, temporaries and contractors in the Quintiles and Commercial organizations.
35	Describe the training system users receive above and beyond the general security and privacy awareness training.	RoPR webinars are provided to active users and prospective users on a semi-annual basis, at minimum.
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 with an archiving vendor. The backups are maintained as long as required by legal and regulatory requirements, and subsequently the client is consulted to determine whether the client would like the information destroyed. If destroyed, a certificate of destruction is obtained. Specific records retention schedules • For records with a retention period of ≤ 6 years, the discs must be reviewed for accessibility/readability at 3 years postdate of disc creation. • For records whose retention period is greater than 6 years or indefinite, the discs must be

		reviewed for accessibility/ readability every 5 years postdate of disc creation. • Review of records stored on a CD/ DVD or archive server must be documented in the appropriate tracking spreadsheet/database at the time of review by the Records & Information Management coordinator. • The AC is responsible for requesting destruction approval from Corporate Legal once the designated retention period has concluded following the guidelines set forth in CS_WI_RM037 Final Disposition and Destruction of Records • The Archive Coordinator will notify Legal using Records Destruction Authorization of those records requiring review within two months following the review date.
38	Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical and physical controls.	User identification, passwords, firewalls, encryption, and Public Key Infrastructure (PKI) are employed. Administrative, technical, and physical security controls required for the system are defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev 4, Security and Privacy Controls for Federal Information Systems and Organizations. These controls strengthen the information systems and the environment in which it operates, and are reviewed on an annual basis.
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).	Session Cookies – Yes, collects PII
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-	Yes

	federal government websites external to HHS?	
43a	Is a disclaimer notice provided to users that follow links to websites not owned or operated by HHS?	Yes. http://www.nih.gov/about/disclaim.htm