US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

05/27/2016

OPDIV:

AHRQ

Name:

Registry of Patient Registries

PIA Unique Identifier:

P-9496384-979384

The subject of this PIA is which of the following?

Minor Application (stand-alone)

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

Does the system include a Website or online application available to and for the use of the general public?

Yes

Identify the operator.

Contractor

Is this a new or existing system?

Existing

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

PIA Validation

Describe in further detail any changes to the system that have occurred since the last PIA.

N/A

Describe the purpose of the system.

The Registry of Patient Registries (RoPR) is a database system designed to meet the following objectives: provide a searchable database of existing patient registries in the United States; facilitate the use of common data fields and definitions in the similar health conditions to improve opportunities for sharing, comparing, and linkage; provide a public repository of searchable summary results, including results from registries that have not yet been published in the peer-reviewed literature; offer a search tool to locate existing data that researchers can request for use in new studies; and serve as a recruitment tool for researchers and patients interested in participating in patient registries.

A patient registry is an organized system tht uses observational study methods to collect uniform data (clinical and other) to evaluate specified outcomes for a population defined by a particular disease, condition, or exposure, and that serves a predetermined scientific, clinical, or policy purpose(s). Examples of individual researcher-generated registries can be found at the AHRQ Registry of Patient Registries, available at https://patientregistry.ahrq.gov.

Registry of Patient Registries (RoPR) gets its data from records classified as 'patient registry' on ClinicalTrials.gov. In addition, registrars of these records may include additional detail pertinent to the RoPR criteria for data collection.

Describe the type of information the system will collect, maintain (store), or share.

RoPR collects metadata, a set of data that describes and gives information about other data, on patient registries, from patient registry record owners. As patient registries are not obligated by law to disclose information, record owners voluntarily submit information to the RoPR to promote collaboration, reduce redundancy, and improve transparency in registry research. Administrative information consisting of an e-mail address is collected from the patient registry record owner, and is not disseminated . This administrative information is 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. 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 Uniform Resource Locator, or URLs. The administrative information is mandatory however, the publicly available information is voluntary. The RoPR is accessible to the public via the internet.

There is no authentication necessary when accessing the RoPR via internet. It supports browser-based internet access and is located at www.patient-registries.ahrq.gov. Users looking to create new RoPR records, or update existing records require user credentials, comprised of their host organization name, username and password in order to control system access. Users browsing material on the RoPR do not require user authentication. The primary users of the system are government agencies and members of the public who are interested in patient registries. Government agencies include funding agencies; government, regulatory, and public health agencies. Members of the public include: pharmaceutical and device manufacturers; biomedical journal editors; patients and healthcare consumers; healthcare payers; healthcare providers; healthcare professional associations; and researchers.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

RoPR is accessible to members of the public who browse the website. The web site can be accessed via the internet using a web browser. Record holders who input and update registry information in RoPR require user credentials, comprised of their host organization name, username and password in order to control system access at www.ClinicalTrials.gov. The RoPR team has worked with the ClinicalTrials.gov team at the National Library of Medicine to ensure session connections are properly restricted. Following authenticating into ClinicalTrials.gov secure area, Protocol Registration & Results System (PRS), the user is led to the secure session authentication gateway of the RoPR, called the Registry Registration System (RRS), where users can enter data into the RoPR system. Once the user reaches RRS, there is no username or password requested as it is not necessary for the users' identity to be verified upon entry to RRS. The secure connection is maintained between the ClinicalTrials.gov white-listed IP addresses and the RoPR system.

A whitelist is a list or register of entities that are being provided a particular privilege, service, mobility, access or recognition. Entities on the list will be accepted, approved and/or recognized.

System administrators and developers who upkeep and configure operations of the system have user credentials and may authenticate only to RRS to access the RoPR as they do not have permissions to access ClinicaTrials.gov PRS system.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name

E-Mail Address

Phone Numbers

Web URL

User Credentials (username, password)

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Public Citizens

Vendor/Suppliers/Contractors

Patient registrars, which include corporations and research organizations who are not business partners/contacts/vendors/suppliers/or contractors of the RoPR; system administrators & developers government agencies and members of the public who are interested in patient registries. Government agencies include funding agencies; government, regulatory, and public health agencies. Members of the public include: pharmaceutical and device manufacturers; biomedical journal editors; patients and healthcare consumers; healthcare payers; healthcare providers; healthcare professional associations; and researchers.

How many individuals' PII is in the system?

500-4,999

For what primary purpose is the PII used?

Administrative PII, which consists of an e-mail address, is used by the agency to contact the record holders regarding the maintenance of their records. Publicly available PII, which consists of record holders' name, e-mail address, telephone number and website URLs, allows the general public to contact the record holder for additional information about the patient registry.

Describe the secondary uses for which the PII will be used.

There are no secondary uses for which the PII will be used.

Identify 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.

Are records on the system retrieved by one or more PII data elements?

No

Identify the sources of PII in the system.

Online

Government Sources

Within OpDiv

Other Federal Entities

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

OMB Control #0935-0203, expires on March 31, 2019.

Is the PII shared with other organizations?

Yes

Identify with whom the PII is shared or disclosed and for what purpose.

Within HHS

PII (First/Last Name) and Title fields are non - mandatory entries, which are indicated as optional fields as a user completes the RoPR profile. This information is available publically for intended uses as identified by the accompanying categories detailing the sponsor's reasons for being contacted. In this case, the Privacy Act is not applicable, however the collection of PII is deemed necessary for collection on the RoPR, for the following reasons: The RoPR is an information repository which connects patient registries with individuals interested in learning more about them and how they advance healthcare. Many patient registries find it mutually beneficial to provide primary contact information to facilitate dialogue between them and interested parties. Patient registries comprise a highly specialized field. Only a subset of the general public would be interested in pursuing dialogue with a particular patient registry, motivated by interest in specific medical conditions being examined. Extra security measures have been taken so that PII is not searchable on the RoPR, in the live or administrative environments.

Registration burden is reduced by clearly indicating that the submission of PII, First Name/Last Name, of the primary contact person purely voluntary, for the purpose of knowledge exchange between the patient registry and concerned members of the public.

Other Federal Agencies

Publicly available PII is disclosed to allow the general public to contact the record holder for additional information about the patient registry.

State or Local Agencies

Publicly available PII is disclosed to allow the general public to contact the record holder for additional information about the patient registry.

Private Sector

Publicly available PII is disclosed to allow the general public to contact the record holder for additional information about the patient registry.

As the sub-contractor, Quintiles is tasked with provisioning system administrators and developers, who perform system maintenance and updates to the RoPR. They have access to PII stored in the RoPR database but are not authorized to create new records, or make updates to existing records on the live RoPR system. The Interconnection Security Agreement (ISA) makes mention of Quintiles as the L&M Policy Research's sub-contractor and its Security Network/ Resource Password Policy/Computer System Account Standards.

Describe any agreements in place that authorizes the information sharing or disclosure.

The purpose of the Memorandum of understanding is to establish a management agreement between the Agency for Healthcare Research and Quality (AHRQ) and contractor, L&M Policy Research, regarding the development, management, operation, and security of the Registry of Patient Registries (RoPR), owned by AHRQ. This agreement will govern the relationship between AHRQ and L&M Policy Research, including designated managerial and technical staff, in the absence of a common management authority and the Inter-connection Security Agreement.

The purpose of the Interconnection Security Agreement (ISA) is to state the requirements for interconnection between the Agency for Healthcare Research and Quality (AHRQ) and ClinicalTrials.gov, for the express purpose of exchanging data between Registry of Patient Registries (RoPR), owned by AHRQ, and registry users using National Library of Medicine's Protocol Registration System (PRS), via the RoPR Registry System (RRS). The interconnection between RoPR, owned by AHRQ, and National Library of Medicine's Protocol Registration System (PRS), owned by ClinicalTrials.gov, is a one-way path. The ClinicalTrials.gov Identifier (NCT ID) and data populating the short and long descriptions in RoPR are transferred from ClinicalTrials.gov.

Describe the procedures for accounting for disclosures

Individuals registering patient registries via the RoPR are told the purposes for which this information (e.g., e-mail) is collected, in accordance with the Privacy Act, not to be used, or disclosed for any other purpose than for the RoPR. To this effect, a disclaimer statement is clearly stated within the RoPR system: “This email will only be used by RoPR and will not be distributed.”

The RoPR record owner has the option to select “Do not contact” on the RoPR. This selected option does not exempt the RoPR user from having to complete these “mandatory” fields: Reasons for being contacted; Organization; E-mail and Phone.

A complaint process is available for individuals who believe their PII has been inappropriately obtained, used, or disclosed, or that their PII is inaccurate.

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 agreements in place (MOU and ISA) govern the management of RoPR’s operations and its existing connection(s) with ClinicalTrials.gov/ PRS. The RoPR registration interface collects the e-mail address of the RoPR record owner. This information is mandatory and is not made public. It is used only for periodic auto-generation of e-mail reminders pertaining to the maintenance of RoPR patient registry data. There is no human administrator that is pulling this information for the purpose of sending out e-mails. Therefore, individuals registering patient registries via the RoPR are told the purposes for which this information (e.g., e-mail) is collected, in accordance with the Privacy Act, not to be used, or disclosed for any other purpose than for the RoPR. To this effect, a disclaimer statement is clearly stated within the RoPR system: “This email will only be used by RoPR and will not be distributed.”

Is the submission of PII by individuals voluntary or mandatory?

Voluntary

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 RoPR record owner has the option to select “Do not contact” on the RoPR. This selected option does not exempt the RoPR user from having to complete these “mandatory” fields: Reasons for being contacted; Organization; E-mail and Phone. PII (First/Last Name) and Title fields are non -mandatory entries, and are indicated as optional fields when the RoPR record owner completes the RoPR profile. This information is available publically for intended uses as identified by the accompanying RoPR categories detailing the sponsor’s reasons for being contacted. In this case, the Privacy Act is not applicable, however the collection of this PII (First/Last Name) is deemed necessary for collection on the RoPR, the RoPR is information repository which connects patient registries with individuals interested in learning more about them and how they advance healthcare.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

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. The change control process will include the specifics regarding collection of PII. Any changes related to notification and consent 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 four (4) years of inactivity.

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.

Administrative PII, which consists of an e-mail address, is used by the agency to contact the record holders regarding the maintenance of their records.

A complaint process is available for individuals who believe their PII has been inappropriately obtained, used, or disclosed, or that their PII is inaccurate. The registry holder may contact the RoPR support team with any concerns. The registry holder may also update their PII on the registry record themselves, as necessary.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

No processes are in place for periodic reviews of PII contained in the system. Data checks by the registry holder are completed before information is posted. The user confirms via check box that all information is accurate to the best of their knowledge; and is responsible for ensuring continued accuracy after submission.

Identify who will have access to the PII in the system and the reason why they require access.

Users:

Registry holders have full access to any PII they provide to update or correct their registry record. Members of the general public may view any PII intended and published for public consumption (but they may not edit published PII).

Administrators:

Any PII entered which is publicly viewable may be viewed by an administrator accessing the RoPR system for maintenance/update purposes.

Developers:

Any PII entered which is publicly viewable may be viewed by an developer accessing the RoPR system for maintenance/update purposes.

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”).

Quintiles Corporate Policy QCP_RB_CDP0005 is corporate-specific, not application specific.

Although it applies to all employees, contractors and temporary staff, globally, this does not mean that contractors are hired and allocated to RoPR system administration or developing responsibilities and are accessing the RoPR system. Therefore, "Contractors" is not applicable.

The categories of individuals described, should have access to PII maintained in the system as PII collected voluntarily is published on the public-facing RoPR website.

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.

Access to the RoPR administrative environment and to RoPR servers is restricted to specific IT personnel such as system administrators and developers tasked with maintaining and updating RoPR systems. User credentials to RoPR systems is by encrypted key-based authentication; all non-secure modes of access are disabled. 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.

There are no special system controls that limit a system administrator's or developer's to the type, amount, or categories of PII necessary to perform their job functions. Therefore, administrative user credentials are provided on task need only and deactivated when the need is no longer there.

In addition, no human administrator is pulling PII information for the purpose of sending out reminder e-mails. PII on the RoPR system cannot be searched for using a keyword or field query search.

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.

Describe training system users receive (above and beyond general security and privacy awareness training).

N/A

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

RoPR patient registry records left inactive for 5 years are archived on the RoPR system.

The PII collected is stored in the secure RoPR database. Per Quintiles' record retention policy: Data 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.

Per Quintiles' record retention policy: 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 Quintiles standard operating procedure, 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.

NARA's Records Control Schedule (RCS) Job Numbers or General Records Schedules (GRSs) is non-applicable to the PII maintained in the RoPR system.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

PII will be secured in the RoPR system using registry holder user credentials (username and password). The authentication process is protected using technical controls such as firewalls, encryption, and Public Key Infrastructure (PKI) methods.

Technical security controls are required for logging into the ClinicalTrials.gov PRS 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.

From a system administrative and maintenance perspective, PII is also secured on administrative user credentials issued based on the need to know and job responsibilities concerning the RoPR.

Identify the publicly-available URL:

https://patientregistry.ahrq.gov

Note: web address is a hyperlink.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Session Cookies that collect PII.

Session cookies captures session identification that doesn't personally ID the user, and identifies the geographical region is collected.

Does the website have any information or pages directed at children under the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

Yes

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

Yes