RHSCIR DATA
USE AND DISCLOSURE POLICY

Table of Contents

1. Introduction

The Praxis Spinal Cord Institute (Praxis) operates in multiple jurisdictions to achieve its mission “To lead collaboration across the global spinal cord injury (SCI) community by providing resources, infrastructure and knowledge; and to identify, develop, validate and accelerate the translation of evidence and best practices to reduce the incidence and severity of paralysis after SCI, improve health care outcomes, reduce long-term costs, and improve the quality of life for those living with SCI”.

In doing so, Praxis is compliant with Canadian legislative requirements, international data protection standards, and privacy best practices.

2. Purpose

The purpose of the *RHSCIR Data Use and Disclosure Policy* is to ensure that the use and disclosure of national RHSCIR data [i.e., data from the Rick Hansen Spinal Cord Injury Registry (RHSCIR) in the custody of Praxis] supports Praxis’ mission, is managed consistently, and is carried out in compliance with Praxis’ privacy and security obligations.

3. Scope

This policy outlines the data access request and approval process at Praxis applicable to requestors seeking to gain access to national RHSCIR record-level data in the custody of Praxis. This policy also ensures that strict technical and administrative controls are in place to facilitate access to national RHSCIR data for authorized purposes while still maintaining effective privacy protection.

This policy applies to:

1. Use of record-level national RHSCIR data by internal data users; and
2. Disclosure of record-level national RHSCIR data by Praxis to internal and external requestors.

This policy does not apply to:

1. Use and disclosure of aggregate national RHSCIR data by Praxis; and
2. Use and disclosure of a facility/site’s own local RHSCIR data.

Use and disclosure of record-level national RHSCIR data must comply with the principles and procedures set forth in this policy and in accordance with applicable laws and agreements.

4. Definitions and Abbreviations

Aggregate Data: Data that has been compiled from record-level data to a level of aggregation that ensures that the identity of individuals cannot be determined by reasonably foreseeable methods (for example, the aggregation satisfies the rules about small cell sizes, and no other data set can reasonably be expected to be available to combine with the data and re-identify the individual).

Data Extract: Data prepared for disclosure to a requestor under a Research Agreement.

Data Sharing Agreement: Agreement between Praxis and the disclosing RHSCIR Site that sets out the data expectations and obligations of each party.

De-identifying: The process of removing identifiers from data in a way that minimizes the risk of an individual’s identity being connected to data. Depending on the level of de-identification used there is always a varying risk of potentially re-identifying the individual. For example, by matching a date of injury to health records.

Disclosure: Release of data, other than to the disclosing Facility/Site or the individual to whom the data pertains, in response to data access requests.

External Requestors: Requestors not affiliated with a RHSCIR Facility/Site Investigator.

Facility/Site: The term ‘facility’ is synonymous with an acute care, rehab, or integrated acute care and rehab hospital. A ‘site’ is a collection of one or more facilities in a geographical region and generally consists of facilities providing the continuum of care from first response and acute care to rehabilitation. The four sites of the Greater Toronto Area (GTA) and the two sites in New Brunswick (NB) are an exception to this definition as each GTA and NB facility provides only acute or rehab care but is still considered a site

Facility/Site Investigators: The persons that contributed data to the requested national RHSCIR data extract and are named in the RHSCIR Data Sharing Agreement with Praxis.

Highly Identifying Data Elements: In the context of this policy: participant / surrogate / next of kin / other contact name, detailed address including city and six-digit postal code, provincial health number, alternative ID number (such as military or prison ID number), hospital chart/encounter number and full date of birth.

Health System Use: The use of health data for clinical program management (i.e., improving front-line health care programs and services), health system management (i.e., improving the effectiveness and efficiency of the health care system), monitoring public health (i.e., understanding the health of the public), and research (i.e., identifying improvements to medical treatments and programs of care, or to better understand the health of the population, the factors influencing health, and the performance of the health care system), all of which lead to improved patient care and health outcomes.

Internal Data Users: Praxis personnel that need data access to perform their assigned duties.

Internal Requestors: RHSCIR Facility/Site Investigators and their affiliates, and researchers employed by Praxis.

National RHSCIR Data: Data from the Rick Hansen Spinal Cord Injury Registry (RHSCIR) submitted to and stored by Praxis.

Population Data BC: A unit of the University of British Columbia which provides on behalf of Praxis, as a service provider, secure storage and secure remote access to project-specific data extracts.

Population Data BC’s Secure Research Environment (SRE): Population Data BC’s central server accessible only via an encrypted Virtual Private Network (VPN) through a firewall and use of a secure access token for two-factor authentication, that hosts RHSCIR data extracts, provides purchasing/licensing software for analysis and ensures that all necessary precautions with respect to data privacy and security are met.

Record-Level Data: Data in which each record is related to a single individual.

Research Agreement: Agreement between Praxis and requestor that sets out the expectations and obligations of each party.

Requestors: Internal and external requestors.

Praxis Personnel: Staff, consultants, contract employees, and volunteers involved in administering and/or managing work for Praxis whether inside or outside Praxis’ premises.

RHSCIR Data: RHSCIR data refers to data about an individual that is related to the individual’s health or the provision of health services to the individual, as collected under the auspices of the Rick Hansen Spinal Cord Injury Registry (RHSCIR).

RHSCIR Data Access Committee (DAC): One of the two committees that reviews data requests. This committee is comprised of the Facility/Site Investigators. Each DAC member must decide, with respect to accessing data requested of their facility/site, whether to approve or reject the access.

RHSCIR Data Executive Scientific Committee (DESC): One of the two committees that reviews data access requests. This committee ensures that applications respect each applicable facility/site’s contribution to the data; applications have been peer-reviewed or demonstrate reasonable merit (e.g., scientific and/or public benefit); and proposed projects will not duplicate other projects in progress using RHSCIR data.

RHSCIR Data Steward: The person designated by Praxis with responsibility for oversight of RHSCIR data.

Use: Involves the handling of RHSCIR data by internal data users who require access in order to perform their assigned duties.

5. Responsibilities

The person at Praxis responsible for receiving and processing all requests through to project completion for RHSCIR data access (use and disclosure) is the RHSCIR Data Steward (further details can be found in "RHSCIR Data Steward Terms of Reference"). The RHSCIR Data Steward may delegate these responsibilities as appropriate. The RHSCIR Data Steward is responsible for ensuring compliance with this policy.

The *national RHSCIR data access request and approval process* is triggered for all internal and external record-level data access requests. Therefore, requestors must be familiar with, and adhere to, this policy.

Once a national RHSCIR data access request is approved by the RHSCIR Data Steward, the application must be approved both by the RHSCIR Data Executive Scientific Committee and the RHSCIR Data Access Committee (further details can be found in "RHSCIR Data Executive Scientific Committee Terms of Reference" and "RHSCIR Data Access Committee Terms of Reference").

Population Data BC, acting as service provider of Praxis, is responsible for providing secure storage and secure remote access to project-specific data extracts according to the terms of the information sharing agreement between Praxis and Population Data BC and the Research Agreement between Praxis and the requestor.

6. Description

6.1 Use of National RHSCIR Data by Internal Data Users

The RHSCIR Data Steward is responsible for access to internal data users in line with Praxis policies and procedures (e.g., based on the 'principle of least privilege') and informing them of additional obligations that may exist (e.g., RHSCIR data from British Columbia and Nova Scotia that is deemed to be personal information must be accessed only within Canada).

Internal data users are Praxis personnel who require access to record-level national RHSCIR data to perform their assigned data management duties, including:

- data quality control (i.e., accuracy, completeness and timeliness of data),
- data transformation, validation, extraction and warehousing [e.g., profiling the data for rule generation and testing in the writing of the data extract, transform and load (ETL) procedures and queries used to process, transform and output the data to alternate schemas for data staging in the data warehouse, and for data delivery through tables, OLAP cubes (Online Analytical Processing Cubes - a method of storing data in a multidimensional form, generally for reporting purposes) and reports and creating analytical data sets in software external to the data warehouse],
- creation of data summaries that fit within the ethics approved, patient consented permitted purpose(s) as per the RHSCIR protocol, for dissemination to the Praxis network and the public (e.g., a RHSCIR annual report, an enquiry relating to the yearly incidence of SCI in Canada, a white paper relating to one of Praxis' operating goals, summary reports to be provided to researchers and clinicians at RHSCIR sites), and
- data analyses for approved data access requests.

Praxis expressly forbids the use of data for anything other than official Praxis business.

Internal data users granted access privileges to national RHSCIR data are responsible for their actions while carrying out these privileges and are monitored by the RHSCIR Data Steward.

Prior to being granted access to record-level national RHSCIR data, internal data users will have completed:

- Praxis' legally binding Confidentiality Agreement; and
- Information privacy and security training and awareness.

Additionally, those with access to the data elements marked as highly identifying [i.e., participant / surrogate / next of kin / other contact name, detailed address including city and six-digit postal code, provincial health number, alternative ID number (such as military or prison ID number), hospital chart/encounter number and full date of birth], will have:

- Satisfied a criminal history check.

6.2 Disclosure of National RHSCIR Data to Requestors

Praxis is committed to supporting the disclosure of national RHSCIR data for health system use.

In responding to RHSCIR data access requests, Praxis:

- Aims to make timely and accurate national RHSCIR data available to requestors consistent with Praxis' mission, applicable laws and agreements, and as per the ethics approved RHSCIR protocol or other ethics approved research protocol;
- May charge requestors for its time in preparing and delivering national RHSCIR data for approved data access requests on a cost recovery basis and the cost of Population Data BC accounts[1];
- Will make reasonable efforts to provide the minimum amount of data with the highest degree of data de-identification, while still fulfilling the purpose identified by the requestors and balancing the risk of re-identification;
- Will ensure the following highly identifying data elements will not be released to requestors: participant / surrogate / next of kin / other contact name, detailed address including city and six-digit postal code, provincial health number, alternative ID number (such as military or prison ID number), hospital chart/encounter number and full date of birth; and
- Requires legally binding agreements with requestors and all individuals requiring access to de-identified data.

Requestors are permitted to gain access to national RHSCIR data for the following five ethics approved, patient consented permitted purpose(s) described in the RHSCIR protocol:

- Clinical Support and Management: To promote, encourage and develop an efficient and effective national health data retrieval and management reporting service.
- Research Support: To create a clinical and epidemiological based information service in order to promote collaboration between scientists and clinicians, and support true translational research, as well as provincial/territorial, national and international data exchange and collaboration.
- Partnerships and Quality Improvement: To demonstrate flexibility in helping partners to achieve their SCI information goals.
- Quality Data and Information: To ensure the quality of data stored in the national RHSCIR database.
- Business Planning and Development: To remain current with changing trends and issues in health care management.

Applications that fall outside the scope of the permitted purposes listed above must develop and obtain ethics approval for their research protocol before access can be provided. For example, proposed data analyses related to a proposed research project involving new data and/or new data linkages in

[1] For more information, refer to "Costs for Data Access Requests".

combination with RHSCIR data must undergo ethics approval in addition to approval by the RHSCIR Data Executive Scientific and RHSCIR Data Access Committees in order to gain approval for the disclosure.

6.2.1 *National RHSCIR Data Access Request and Approval Process*

6.2.1.1 Process Flow

All internal and external requests for national RHSCIR data are subject to the following process flow, supported further in the step-by-step procedures in section 6.2.1.2.:

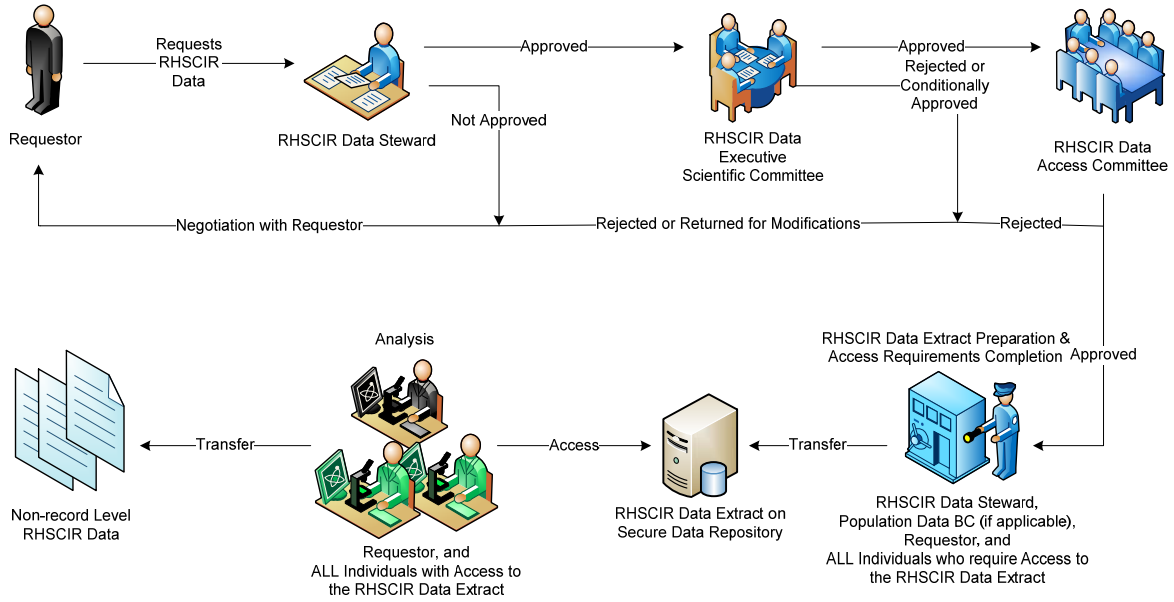

Figure: National RHSCIR Record-Level Data Access Request and Approval Process Flow

6.2.1.2 Step-by-Step Procedures

Step 1: Requestor Completes and Submits an Application

The first step of the data access request and approval process requires the requestor to:

1. Complete an *Application for Disclosure of National RHSCIR Data*; and
2. Submit the application to the RHSCIR Data Steward.

Step 2: RHSCIR Data Steward Reviews the Application

The RHSCIR Data Steward reviews the application, coordinates with the requestor and committees involved in the approval process, and establishes timelines and constraints.

The RHSCIR Data Steward reviews the application for completeness and considers whether:

- The request is consistent with Praxis' mission, applicable laws and agreements;
- The request is consistent with the permitted purposes described in the approved RHSCIR protocol or ethics approval for their research protocol will be obtained before access is provided; and
- It is feasible for Praxis to provide the data requested (e.g., availability of data elements requested, resource requirements).

The RHSCIR Data Steward then determines whether to:

1. Initially approve the application (and proceed to Step 3); or
2. Negotiate with the requestor as required; or
3. Reject the application.

The RHSCIR Data Steward liaises with additional Praxis personnel (e.g., Privacy Officer, research personnel) as required.

Step 3: RHSCIR Data Executive Scientific Committee Reviews Application

The DESC considers the following criteria when reviewing applications approved by the RHSCIR Data Steward:

- If the application respects the individual facility/site contributions;
- If the application, as applicable, has been peer-reviewed or demonstrates reasonable merit (e.g., scientific and/or public benefit); and
- If the proposed project will not duplicate other projects in progress using national RHSCIR data.

The DESC determines whether to:

1. Approve the application (and proceed to step 4); or
2. Grant conditional approval; or
3. Reject the application.

Where the DESC approves the application, it is forwarded to the DAC.

Where conditional approval is granted, the application is returned to the RHSCIR Data Steward along with conditions for resubmission, which is then returned to the requestor who may resubmit a revised application.

Step 4: RHSCIR Data Access Committee Reviews Application

The Facility/Site Investigators that contributed data to the requested data extract and are named in the RHSCIR Data Sharing Agreement with Praxis, who make up the members of the DAC, are made aware of the application via email from the RHSCIR Data Steward. The email will detail the outline of the request, requestor details, and relevant comments from the DESC.

The Facility/Site Investigators may request more information, the entire application if they wish, which will be anonymized except for the names of the requestors and their respective institutions/organizations. The Facility/Site Investigators, with respect to access to the data requested of their facility/site, will decide whether to:

1. Approve the access (and proceed to step 5); or
2. Reject access.

Where the application is rejected, it is returned to the RHSCIR Data Steward along with the reason(s) for rejection, which is then returned to the requestor who may resubmit a revised application.

Step 5: National RHSCIR Data Extract Preparation & Access Requirements Completion

The RHSCIR Data Steward will extract the necessary national RHSCIR data from the data warehouse or analytical data sets and complete any programming derivation steps and documentation procedures (e.g., data specifications document and annotated case report forms) required as per the application. Any data elements marked as highly identifying [i.e., participant / surrogate / next of kin / other contact name, detailed address including city and six-digit postal code, provincial health number, alternative ID number (such as military or prison ID number), hospital chart/encounter number and full date of birth] will be removed.

Reasonable efforts will be made to provide the minimum amount of data with the highest degree of data de-identification, while still fulfilling the purpose identified by the requestors and balancing the risk of re-identification. During this step in the process, the RHSCIR Data Steward will consider issues and take steps to ensure that the privacy and security of the data is maintained.

Then one of the following steps will be followed:

A. For projects not analyzed by Praxis personnel where data will be accessed via Population Data BC's Secure Research Environment:

- Praxis and the requestor will complete a legally binding Research Agreement.
- The RHSCIR Data Steward will forward the Research Agreement along with a copy of the original application to Population Data BC to confirm that the project has been approved.

- Population Data BC will then directly contact the requestor to sign a Secure Research Environment (SRE) Storage Agreement and pay the amount allotted in the cost quote provided where applicable.
- After the SRE Storage Agreement has been signed by the requestor and the payment has been received by Population Data BC, individuals requiring access to the national RHSCIR data extract will sign the Confidentiality Pledge, Token Terms of Use and complete the online privacy training.

B. For projects not analyzed by Praxis personnel where data will be accessed via a Secure Data Repository (a service provider that provides secure storage and secure remote access (if required) to project-specific data extracts, normally Population Data BC's SRE for projects not analyzed by Praxis personnel, or Praxis' Designated Network Server for projects analyzed by Praxis personnel) other than Population Data BC's Secure Research Environment:

- *For data extracts not de-identified to a level of zero or near zero risk of re-identification:*
    - Praxis and the requestor will complete a legally binding agreement (such as a Data Sharing Agreement or similar).
- *For data extracts de-identified to a level of zero or near zero risk of re-identification:*
    - Requestors will complete Praxis' legally binding Confidentiality Agreement.
- The RHSCIR Data Steward will forward the agreement to the relevant organization to confirm that the project has been approved.
- Any relevant specific organizational policies and procedures will be followed prior to secure data transfer.

C. For projects analyzed by Praxis personnel:

- Prior to being granted access to the national RHSCIR data extract, Praxis personnel will have completed:
    - Praxis' legally binding Confidentiality Agreement; and
    - Information privacy and security training and awareness.

Once the above steps are complete, the national RHSCIR data extract will be validated (through code review, independent programming or output review as appropriate to the complexity of the request) and transferred securely by the RHSCIR Data Steward to a project specific folder on a Secure Data Repository.

Step 6: RHSCIR Data Extract Access

Individuals who access the RHSCIR data extract are not permitted to transfer any record-level data, whether the full data extract or subsets of the data extract from their project-specific folder on the Secure Data Repository, unless granted permission by the RHSCIR Data Steward. They are also not allowed to upload data not specified in the application. However, they are allowed to transfer files not containing record-level data (aggregated results of analysis, programming scripts, documentation without personal information) into and out of their project-specific folder. Activities on the Secure Data Repository are generally logged and monitored.

Step 7: RHSCIR Data Extract Destruction

For projects not analyzed by Praxis personnel and for data extracts not de-identified to a level of zero or near zero risk of re-identification: Upon termination of the Research Agreement, all accounts and access to the data on the SRE will be disabled, and the project closure process will be completed. The requestor may apply to Praxis to extend the Research Agreement.

For projects analyzed by Praxis personnel and *for data extracts de-identified to a level of zero or near zero risk of re-identification:* The data will be securely destroyed upon project completion or cessation as outlined in Praxis' *Data Storage, Retention and Destruction Policy*.

6.2.1.3 Rejected Applications and Applications Returned for Modification

If the RHSCIR Data Steward, DESC, or DAC grant conditional approval or reject an application, the RHSCIR Data Steward informs the requestor of the decision and the reason(s) for granting conditional approval or rejecting the application/access to data.

Applications may then be re-submitted to the RHSCIR Data Steward provided modifications have been made to the application in accordance with the conditions imposed.

Requestors have a right of appeal to the decisions of the RHSCIR Data Steward to the DESC.

6.2.1.4 Timelines

Praxis endeavours to provide a timely response to all data access requests, but gives priority to internal requestors.

6.3 Breach of this Policy

Violations of this policy may result in the loss of data access privileges, and appropriate disciplinary action, including the termination of employment or other relationship with Praxis.

Exceptions to this policy must be documented (to allow for issues in the policy to be identified and information to be submitted in the event of an audit/investigation, etc.).

6.4 Review of this Policy

This policy will be reviewed at least every two (2) years and revised by Praxis as required.

7. References

Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research Council of Canada, Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans, December 2014.

Canadian Institutes for Health Research (CIHR) Best Practices for Protecting Privacy in Health Research, September 2005.

Health System Use Technical Advisory Committee Data De-Identification Working Group, 'Best Practice' Guidelines for Managing the Disclosure of De-Identified Health Information, October 2010.

Canadian Institute for Health Information (CIHI), Privacy Policy on the Collection, Use, Disclosure and Retention of Personal Health Information and De-Identified Data (Bilingual), June 2009.

Cancer Care Ontario, Data Use & Disclosure Standard, July 2014.

Canada Health Infoway/Pan-Canadian Health Information Privacy Group, Privacy and EHR Information Flows in Canada: Common understandings of the Pan-Canadian Health Information Privacy Group, Version 2.0, July 31, 2012.

QA-POL-004: Information Privacy and Security Standard of Conduct.

QA-SOP-003: Privacy Breach Management Protocol.

QA-POL-003: Data Storage, Retention and Destruction Policy.

IT-SOP-014: Information Security Incident Management Procedure.

Praxis Access Agreement for personal information from BC subject to FIPPA and from NS subject to PIIDPA.

RHSCIR Data Steward Terms of Reference.

RHSCIR Data Executive Scientific Committee Terms of Reference.

RHSCIR Data Access Committee Terms of Reference.

Costs for Data Access Requests.

8. Attachments

Not applicable.