Systems Privacy Policy

Contents

Systems Privacy Policy .............................................................................................................. 1
  Introduction ............................................................................................................................ 2
  Use of REDCap ...................................................................................................................... 2
  Identifiable Information ........................................................................................................... 2
    TCPS Classification ............................................................................................................. 2
    Examples of Identifiers ........................................................................................................ 2
  CIHR Best Practices ............................................................................................................... 4
  Alberta Health Services ......................................................................................................... 4
  External Researchers ............................................................................................................ 4
  WCHRI Policy ......................................................................................................................... 4
    Systems Security (General) .................................................................................................. 4
    For Researchers ................................................................................................................... 4
    Obligations Under the Health Information Act ................................................................. 6
    Policy Implementation ....................................................................................................... 6
  References ............................................................................................................................. 7
  Appendix A - REDCap Security Settings and Features ........................................................... 8
    Operating Environment ....................................................................................................... 8
    Application Security Features ............................................................................................. 8
  Appendix B – Two Factor Authentication ............................................................................ 10
    Our Approach .................................................................................................................... 10
    Which Projects Require 2FA? .............................................................................................. 10
  Related Documents ............................................................................................................... 10
  Authorization ......................................................................................................................... 10
Introduction
Ethical considerations and both federal and provincial legislation require that identifiable research study data be subject to appropriate administrative and technological protection. Whilst this is primarily the responsibility of the Principal Investigator WCHRI recognizes that, as a systems provider, it has a role to play regarding data security and privacy. This document provides advice to the researchers and documents WCHRI’s approach to data security and privacy.

Use of REDCap
The University of Alberta licenses REDCap for internal not-for-profit use only. It is provided free of charge to University of Alberta researchers and their collaborators.

Identifiable Information
The Tri Council Policy Statement (TCPS 2) defines identifiable information as follows:

Information that may reasonably be expected to identify an individual, alone or in combination with other available information, is considered identifiable information…

It goes on to further categorize identifiable information.

TCPS Classification
- **Directly identifying information** – the information identifies a specific individual through direct identifiers (e.g., name, social insurance number, personal health number).
- **Indirectly identifying information** – the information can reasonably be expected to identify an individual through a combination of indirect identifiers (e.g., date of birth, place of residence or unique personal characteristic).
- **Coded information** – direct identifiers are removed from the information and replaced with a code. Depending on access to the code, it may be possible to re-identify specific participants (e.g., the principal investigator retains a list that links the participants’ code names with their actual name so data can be re-linked if necessary).
- **Anonymized information** – the information is irrevocably stripped of direct identifiers, a code is not kept to allow future re-linkage, and risk of re-identification of individuals from remaining indirect identifiers is low or very low.
- **Anonymous information** – the information never had identifiers associated with it (e.g., anonymous surveys) and risk of identification of individuals is low or very low.

Examples of Identifiers
The US Government’s Health Insurance Portability and Accountability Act (HIPPA)\(^2\) contains useful examples of data items that constitute identifiers. These may be categorized as either direct or indirect identifiers. This categorization is not intended to be definitive but should be considered as guidance for investigators when considering the context of their own study data.
<table>
<thead>
<tr>
<th>Identifier</th>
<th>Direct</th>
<th>Indirect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Study participant names</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Study participant initials</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Medical practitioner names</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Participant’s address (complete)</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>All geographical subdivisions smaller than a province/territory. (This includes complete and partial postal codes).</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>All elements (except year) of dates related to an individual. Age and any element of date of birth for subjects over the age of 90.</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Phone number</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Fax number</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Email addresses</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Social Security numbers</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Medical record and healthcare numbers</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Health plan beneficiary numbers</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Account numbers</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Certificate/license numbers</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Vehicle identifiers and serial numbers, including license plate numbers</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Device identifiers and serial numbers</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Web Universal Resource Locator (URL)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Internet Protocol (IP) address number</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Biometric identifiers, including finger and voice prints</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Full face photographic images and any comparable images</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
CIHR Best Practices

Investigators should be familiar with CIHR best practice guidelines for protecting privacy in health research. These can be summarized as follows:

1) Determining the research objectives and justifying the data needed to fulfill these objectives
2) Limiting the collection of personal data
3) Determining if consent from individuals is required
4) Managing and documenting consent
5) Informing prospective research participants about the research
6) Recruiting prospective research participants
7) Safeguarding personal data
8) Controlling access and disclosure of personal data
9) Setting reasonable limits on retention of personal data
10) Ensuring accountability and transparency in the management of personal data

For more information see the CIHR Best Practices for Protecting Privacy in Health Research, September 2005\(^3\).

Alberta Health Services

The Alberta Health Services standard IPO-2013-0004 also contains recommendations that should be followed by Alberta based clinicians when disclosing health information for research purposes.

External Researchers

Researchers from institutions other than the University of Alberta may be required to comply with additional local requirements.

WCHRI Policy

Systems Security (General)

WCHRI’s systems are housed in a physically secure data centre at the University of Alberta and are behind the Faculty of Medicine’s firewall. Port 443 (SSL) is open to the public internet. Login requires the use of a user ID and password pair over a secure (SSL) connection.

For Researchers

General

1) Researchers must comply with appropriate policies and procedures based on local legislation and institutional requirements. At the University of Alberta this includes:
   a. Research Policy
   b. Research Records Stewardship Guidance Procedure

   A list of research procedures is available from the University of Alberta Research Services Office.

2) Passwords and user accounts must be appropriately managed.
   a. System accounts (login information) must not be shared between multiple users.
   b. Users are accountable for any actions performed under their ID.
   c. User’s computers should be protected against viruses and unauthorized use. (Login enforced and password protected screen savers enabled.)
d. Principal Investigators are responsible for removing a user’s project related privileges if they leave the research team or no longer require access to a project.

e. Institutional email addresses are preferred and users should not use shared email addresses with their REDCap profile.

3) Online training relating to ethics and privacy is available on the TCPS2 web site at http://www.pre.ethics.gc.ca/eng/education/tutorial-didacticiel/

**Storing Identifiers**

WCHRI strongly discourages storage of identifiers in a study database. However some studies may require that identifiers be stored for data matching or administrative purposes. Where this is the case appropriate approvals and consents must be obtained and additional technical safeguards applied.

1) Only the minimum number of identifiers required should be entered into electronic database systems.

2) The project’s ethics application(s) must detail identifiers that are collected and stored in the database and the study team must comply with any conditions imposed by the ethics board(s).

3) Unless consent is waived by Ethics, participants must be appropriately consented and this consent should document how personally identifiable information will be handled.

4) REDCap projects that contain direct identifiers must be enabled for two factor authentication. (See appendix B)

5) Personal identifiers must be flagged in REDCap’s online designer. Export of identifiers must only be allowed for users who require them for data matching purposes (using REDCap’s User rights module).

6) Identifiers are not required for analysis and should be removed from the database once data matching and cleaning is complete.

7) In Alberta, if the Principal Investigator is obtaining health information from a custodian such as Alberta Health Services, then the Principal Investigator must enter into a research agreement with the custodian (as defined in Alberta’s Health Information Act). This agreement must detail how personal identifiers will be collected and stored. This agreement must also identify with whom the personal information may be shared and for what purposes.

**Surveys**

When collecting research data using electronic surveys consent is often implied. However surveys should include an REB approved consent statement indicating that:

1. By completing the form the participant is consenting to the collection and storage of the data

2. The data will be stored in an electronic database and used for research purposes

**Mobile and Third Party Applications**

Some systems, notably REDCap, provide mechanisms by which applications can communicate with the central server in order to retrieve or update data. The following general principals apply to such applications:

1. Only approved applications will be allowed access to data stored on the server.

2. Communications between external applications and the server will be conducted using secure protocols such as SSL.
3. External applications must employ appropriate techniques to secure the data. Typically these will include:
   a. ID and password based login.
   b. Encryption of mobile devices and/or data files.
4. Project managers (typically the Principal Investigator) are responsible for the privacy and security of data that is sourced from University of Alberta and Alberta Health Services systems and must ensure that such data is only accessible to authorized individuals.

**Data Retention**

REDCap is not an archival system. However, study data will remain in the REDCap system until:

1. an authorized member of the study team deletes the project or requests that the project is deleted,
2. REDCap system managers request removal of a completed project from the system, or
3. the system is decommissioned

If required, and prior to deleting a project from the REDCap system, WCHRI personnel will make arrangements with the study team for data to be delivered to the study team for archival. For privacy reasons it should be noted that deleted studies remain in REDCap for 30 days following deletion. Study data will also remain in system backups for a complete backup cycle.

**Obligations Under the Health Information Act**

Some projects that use REDCap may be collecting and storing “identifiable healthcare information”. If this is the case then the researcher is obliged to comply with section 54 of the HIA\(^4\). As employees of the University of Alberta WCHRI staff undertake regular privacy training and are familiar with local privacy legislation. In order to help the researcher meet their obligations under the HIA WCHRI undertakes:

1. Only to access study data for the purposes of providing systems support and/or research services.
2. Not to distribute identifiable healthcare information outside the study team without the Principal Investigator’s permission.
3. Not to contact any research subject without the consent of the Principal Investigator, except in response to a support request received from the research subject.
4. To allow a Custodian, as defined in the HIA, access to WCHRI’s premises in order to confirm compliance with the HIA.

Where a researcher enters into a data disclosure agreement with a Custodian, WCHRI, if requested, will review the agreement and will advise regarding compliance.

**Policy Implementation**

1. This policy document will be made available on the REDCap front page. It will also be referenced during WCHRI hosted training sessions.
2. Principal investigators will be asked to electronically sign a privacy declaration when they apply for a REDCap project. This will confirm that:
   a. Researchers are familiar with policy regarding the storage of direct identifiers within REDCap.
   b. Researchers are familiar with TCPS2 guidelines regarding privacy.
   c. Direct identifiers will/will not be stored within the REDCap project.
   d. Appropriate ethics approval has been obtained and that any identifiers are documented in the ethics application.
References


4. Health Information Act [https://open.alberta.ca/publications/h05](https://open.alberta.ca/publications/h05)
Appendix A - REDCap Security Settings and Features

Operating Environment

WCHRI’s REDCap system resides in a physically secure data centre maintained by the Faculty of Medicine and Dentistry at the University of Alberta. The Faculty uses next-generation firewalls (NGFW) with traditional port filtering and stateful inspection, along with additional enhanced, modern security layers such as:

- Intrusion Protection System (IPS)
- SSL inspection
- Antivirus
- Web Filtering
- Application Control
- Anti-Spam

The application and database are on separate machines. On the application server port 443 (SSL) is open to the public internet. The database server is only accessible from a small number of designated machines within the Faculty’s sub-net.

Access to REDCap is via a standard web browser using 128 bit SSL encryption. All data passing between the browser and server is encrypted. Unencrypted access is not allowed.

Application Security Features.

Study team members login via a login page using an ID and password combination.

The following configurable features are designed to prevent unauthorized access.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login page autocomplete</td>
<td>Disabled</td>
<td>Disabling autocomplete increases security during login, especially for shared computers.</td>
</tr>
<tr>
<td>Number of failed login attempts.</td>
<td>5</td>
<td>After this many login attempts the user cannot login for the specified period.</td>
</tr>
<tr>
<td>Lockout time</td>
<td>15 minutes</td>
<td></td>
</tr>
<tr>
<td>Auto Logout Time.</td>
<td>20 minutes</td>
<td>If users have no activity in REDCap for this amount of time they will get a two-minute warning before being automatically logged out.</td>
</tr>
<tr>
<td>Password complexity</td>
<td>Length &gt;= 10</td>
<td>The password must contain only letters, numbers, and underscores, and it must consist of at least one lower-case letter, one upper-case letter, and one number</td>
</tr>
<tr>
<td></td>
<td>Must contain 3 character types.</td>
<td></td>
</tr>
<tr>
<td>Password change enforced after</td>
<td>90 days</td>
<td>Users must change their passwords at least this often.</td>
</tr>
<tr>
<td>Password re-use limit</td>
<td>5 most recent passwords</td>
<td>During a password change users cannot re-use their most recent passwords.</td>
</tr>
<tr>
<td>Password recovery</td>
<td></td>
<td>Users must answer a security question before their password is reset. This reduces the likelihood of a password reset being initiated from a hacked email account.</td>
</tr>
<tr>
<td>Two Factor Authentication (2FA)</td>
<td>2FA requires users to complete a second authentication process before gaining access to projects containing identifiers. (Appendix B).</td>
<td></td>
</tr>
<tr>
<td>----------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>IP Address Blocking</td>
<td>REDCap automatically blocks IP addresses that exhibit unusual activity. For instance excessive failed login attempts. This is designed to prevent denial of service attacks and automated password hacking attempts (bots).</td>
<td></td>
</tr>
<tr>
<td>Inactive Users</td>
<td>Users who have not logged into their account for six months or more are automatically suspended.</td>
<td></td>
</tr>
<tr>
<td>Electronic Surveys</td>
<td>REDCap may deliver survey invitations to study participants via email. Each invitation contains a token that is unique to that participant. Optionally, once a survey has been completed it is no longer available to the participant and can only be accessed by an appropriately authorized REDCap user.</td>
<td></td>
</tr>
<tr>
<td>Survey Logins</td>
<td>Optionally, study participants may be configured with a “survey login”. This feature requires the user to login using two predefined pieces of information such as a user ID and password.</td>
<td></td>
</tr>
<tr>
<td>Logging</td>
<td>REDCap logs both system level and project level events such as logins, data exports and record updates.</td>
<td></td>
</tr>
</tbody>
</table>
| Project logging                  | REDCap provides project level logging information. In addition to viewing update history for individual records, authorized users can query the project logs for the following logged events:  
  • Data exports  
  • Project design and management  
  • User management  
  • Record creation, update, deletion  
  • Record locking  
  • Electronic signatures  
  • Record (page) views. |
Appendix B – Two Factor Authentication

Two-factor authentication (also known as 2FA) provides unambiguous identification of users by means of the combination of two different components. In REDCap’s case these two components are the user id / password login and a time limited six digit code that is provided to the user by one of the following methods:

- A text message (SMS) to the user’s cell phone
- A voice call to the user’s desk/cell phone
- The Google Authenticator application installed on a mobile device
- An email to the user’s registered email address

Our Approach

WCHRI’s approach to 2FA is designed to provide additional security while being as unobtrusive and simple to use as possible. Key points are as follows:

- 2FA is only enforced on users logging in from devices outside of the MedIT (University of Alberta Faculty of Medicine), Alberta Health Services and other trusted networks.
- 2FA is enabled on a project by project basis

As a result of these two considerations the majority of REDCap users are unlikely to experience 2FA during the course of their regular working day.

Which Projects Require 2FA?

Projects that contain any of the direct identifiers listed above should have 2FA enabled. On our "standard" REDCap installation 2FA is enabled for new projects by default. Investigators may request that 2FA is disabled for their project if they do not consider the project data to be identifiable or otherwise sensitive.

2FA is not yet available on our “validated” REDCap installation.

Additional information can be found on our REDCap support pages at:

http://help.redcap.ualberta.ca

Related Documents

<table>
<thead>
<tr>
<th>Document ID</th>
<th>Document Name / Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOP 2.02</td>
<td>Security and Access</td>
<td>Documents WCHRI’s approach to systems security and access.</td>
</tr>
</tbody>
</table>

Authorization

Submitted by: Rick Watts  
Signature: [Signature]  
Date: 30 Jul 2019

Authorized by: Tanya Voth  
Signature: [Signature]  
Date: July 30 2019