



Title: Privacy Policy	Area: REDCap
	Version No.: 2.0
Owner: WE-SPARK Health Institute	Document Type: SOP
	Initial Issue Date: 01-April-2020
	Effective Date: 01-April-2020
	Pages: 8

1.0 Introduction

Users of REDCap are expected to abide by ethical considerations, our [Terms of Use](#), [TCPS-2](#), as well as both federal and provincial legislation as it applies to the collection, storage and sharing of research data involving humans. It is ultimately the responsibility of the Principal Investigator (PI) and those who have been delegated REDCap roles by the PI to ensure they are PHIPA compliant. However, WE-SPARK serves as the REDCap system administrator we also have a role in securing research data and privacy. This document will help guide researchers and their delegates on WE-SPARK's approach to data security and privacy.

2.0 Persons Affected

All users of the WE-SPARK Health Institute instance of REDCap.

3.0 Use of REDCap

The University of Windsor licenses REDCap for internal and not-for-profit use amongst WE-SPARK Health Institute partners. It is provided free of charge to WE-SPARK Health member institutions. There may be additional partners who are able to access REDCap should they form a formal collaboration with WE-SPARK Health Institute.

4.0 Storing Personal Health Information and Identifiers

4.1 *Storing Identifiers*

Currently, WE-SPARK Health Institute prohibits the storage of direct identifiers **unless they are used for automating workflows (Survey Module, Twilio, etc)** in REDCap projects, and have been approved by the REB.



Title: WE-SPARK REDCap Privacy Policy	Policy No.: REDCap Privacy 2.0
	Page No.: 2 of 8

Direct identifiers should be stored outside of REDCap in a secure format that adheres to local institutional policy. If they are being used for automating workflows, they should be removed once they are no longer needed.

REDCap users **can store indirect identifiers** in their REDCap projects with appropriate approvals from their REB of Record. There is a non-exhaustive list of examples of what constitute direct and indirect identifiers in [Section 9.0](#).

As stated in the Terms of Use, real participant data should not be entered until a project has moved to “Production Status” ([See Production Status SOP](#)). At this time, the REDCap administrator will review the project for the use of direct identifiers. If direct identifier fields are found, the administrator will inform the user of their need to be removed unless they are being used for workflow automation and have REB approval. Any indirect identifier fields found must be approved by the REB.

REDCap users with approval to store indirect identifiers should utilize de-identification to ensure their REDCap project data cannot be linked to their participants in the case of a data breach. It is best practice to generate a Unique Study IDs for all participants in your project. This ID should then be used as the Record ID within REDCap. This reduces likelihood that bad actors could identify study participants if they were able to obtain access to your REDCap project.

For more information on de-identification, please review guidelines created by the Information and Privacy Commissioner of Ontario: <https://www.ipc.on.ca/wp-content/uploads/2016/08/Deidentification-Guidelines-for-Structured-Data.pdf>.

4.2 Surveys

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



Title: WE-SPARK REDCap Privacy Policy	Policy No.: REDCap Privacy 2.0
	Page No.: 3 of 8

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.

4.3 *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 administrators request removal of a completed project from the system, or
3. The system is decommissioned.

Currently, WE-SPARK Health Institute will work with users to navigate possible archival opportunities outside of REDCap.

4.4 *Mobile and Third-Party Applications*

REDCap provides mechanisms by which applications can communicate with the central server to retrieve and update data. The following general principles apply to such applications:

1. Only approved applications will be allowed access to data stored on the REDCap server.
2. Communications between external applications and the server will be constructed 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 WE-SPARK



Title: WE-SPARK REDCap Privacy Policy	Policy No.: REDCap Privacy 2.0
	Page No.: 4 of 8

Health Institute and their partner institutions and must ensure that such data is only accessible to authorized individuals.

5.0 CIHR Best Practices

The Canadian Institute for Health Research provides best practice guidelines for protecting privacy in health research.

<https://cihr-irsc.gc.ca/e/29072.html>

6.0 External Researchers and Collaborators

Researchers and Collaborators from institutions outside of the WE-SPARK Health Institute partnership may request REDCap accounts. To be granted one they must have a WE-SPARK Health Institute researcher sponsor them. There are additional requirements that are highlighted in the [External Researcher and Collaborator SOP](#).

7.0 System Security

REDCap is hosted on a physical server maintained by the University of Windsor Information Technology Services (ITS). The server is secured behind a BigIP F5 application load balancer and the network firewall. The actual server is network locked and only accessible directly within the IT Services network.

The filesystem and database are backed up each morning at 1:00AM.

8.0 User Responsibilities

Responsibilities are highlighted in [REDCap Terms of Use](#).

REDCap users must adhere to the Terms of Use and applicable local institutional requirements. Any REDCap projects that require REB approval should adhere to any applicable policies from the UWindsor REB regarding online data storage, collection, and retention (see [UWindsor REB](#)).



Title: WE-SPARK REDCap Privacy Policy	Policy No.: REDCap Privacy 2.0
	Page No.: 5 of 8

Passwords, accounts, and sponsored accounts must be appropriately managed. **REDCap accounts should not be shared between multiple users.** Every REDCap user requires their own individual account. Users are accountable for any violations performed under their REDCap account. It is important to make sure the computer being used to access REDCap is secure against viruses and unauthorized use.

Users may have REDCap access revoked and face additional consequences based on the severity of the violation.

9.0 Identifiable Information

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

Information is identifiable if it may reasonably be expected to identify an individual, when used alone or combined with other available information.

TCPS Classification of Identifiable Information

- **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 names so data can be re-linked if necessary).
- **Anonymized information** – the information is irrevocably stripped of direct identifiers, a code is not kept allowing future re-linkage, and risk of re-



Title: WE-SPARK REDCap Privacy Policy	Policy No.: REDCap Privacy 2.0
	Page No.: 6 of 8

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



Title: WE-SPARK REDCap Privacy Policy	Policy No.: REDCap Privacy 2.0
	Page No.: 7 of 8

Identifier	Direct	Indirect
Study participant names	X	
Study participant initials		X
Medical practitioner names		X
Participant's address (complete)	X	
All geographical subdivisions smaller than a province/territory. (This includes complete and partial postal codes).		X
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.		X
Phone number	X	
Fax number	X	
Email addresses	X	
Social Security numbers	X	
Medical record and healthcare numbers	X	
Health plan beneficiary numbers	X	
Account numbers	X	
Certificate/license numbers	X	
Vehicle identifiers and serial numbers, including license plate numbers	X	
Device identifiers and serial numbers		X
Web Universal Resource Locator (URL)	X	
Internet Protocol (IP) address number	X	
Biometric identifiers, including finger and voice prints	X	
Full face photographic images and any comparable images	X	

DISCLAIMER: This material has been prepared solely for internal use at WE-SPARK HEALTH INSTITUTE. WE-SPARK HEALTH INSTITUTE accepts no responsibility for use of this material by any person or organization not associated with WE-SPARK HEALTH INSTITUTE. No part of this document may be reproduced in any form for publication without the permission of WE-SPARK HEALTH INSTITUTE. This is a controlled document. Any documents appearing in paper form are not controlled and should always be checked against the electronic version prior to use. The electronic version should always be considered the most current and accurate version.



Title: WE-SPARK REDCap Privacy Policy	Policy No.: REDCap Privacy 2.0
	Page No.: 8 of 8

Date	Revision No.	Revision Type (minor edit, moderate revision, complete revision)	Reference Section(s)
2021-Feb-17	1.0	New procedure drafted	N/A
2021-May-05	2.0	Minor edit Updated language on storing direct identifiers to comply with new Terms of Use (v5)	4.0 Storing Personal Health Information and Identifiers

DISCLAIMER: This material has been prepared solely for internal use at WE-SPARK HEALTH INSTITUTE. WE-SPARK HEALTH INSTITUTE accepts no responsibility for use of this material by any person or organization not associated with WE-SPARK HEALTH INSTITUTE. No part of this document may be reproduced in any form for publication without the permission of WE-SPARK HEALTH INSTITUTE. This is a controlled document. Any documents appearing in paper form are not controlled and should always be checked against the electronic version prior to use. The electronic version should always be considered the most current and accurate version.