

PIA01829 – UBC REDCap Application

PIA REVIEW – EXECUTIVE REPORT



PREFACE

This document forms part of UBC Safety and Risk Services (SRS) PrISM's internal documentation for support and administration of the Privacy Impact Assessment (PIA) Review Process. In particular, it documents the final report of the specified PIA review.

This segment serves to provide and record document control capabilities for this document.

Controlled Document

The template and final report documents are controlled documents. The master electronic versions of each reside on the SRS TeamShare S-drive. Any copies or versions not provided directly by the SRS PrISM team, or which have a broken chain of custody, are not to be considered as official copies.

Document Control

The following sub-sections provide a record of the base document template revision history and control.

CONTRIBUTORS

CONTRIBUTOR	DEPARTMENT	POSITION
Stockman, Christian	Safety and Risk Services	Privacy and Information Security Risk Advisor

Figure 1 - Major Document Revision Approval History

TEMPLATE REVISION HISTORY

REVISION #	DATE	REVISED BY	DESCRIPTION
1.0	2021.04.20	Stockman, Christian	Final draft/edits

Figure 2 - Document Revision History and Revision Summary

TEMPLATE REVISION APPROVAL

REVISION #	DATE	REVISED BY	DESCRIPTION
1.00		Johnson, Susan	Initial release of document

Figure 3 - Major Document Revision Approval History

TABLE OF CONTENTS

PREFACE	i
Controlled Document	i
Document Control	i
Contributors	i
Template Revision History	i
Template Revision Approval	i
TABLE OF CONTENTS.....	ii
TABLE OF FIGURES	iv
PART 1: GENERAL INFORMATION & OVERVIEW	1
1.1 Executive Summary	1
1.2 Description of the Program, System, Application, or Initiative Assessed	2
1.3 Scope of PIA.....	2
1.4 Related PIAs.....	2
1.5 Elements of Information or Data.....	2
1.6 Storage or Access Outside of Canada (including back-ups and recovery).....	3
1.7 Data-Linking Initiative.....	3
1.8 Is this a Common or Integrated Program or Activity?.....	3
PART 2: PROTECTION OF PERSONAL INFORMATION	4
2.1 Personal Information Flow Diagram / Table	4
2.2 Risk Mitigation Table.....	4
2.3 Collection Notice	4
2.4 Consent for Storage/Access Outside of Canada & Opt-Out Procedure (If Any)	4
2.5 Consent Withheld Procedure	4
PART 3: SECURITY OF PERSONAL INFORMATION.....	5
3.1 Physical Security Measures	5
3.2 Technical Security Measures.....	5
3.3 Security Policies, Procedures, and Standards	5
3.4 Tracking Access / Access Controls	5
PART 4: ACCURACY, CORRECTION, AND RETENTION	5
4.1 Updating and Correcting Personal Information	5
4.2 Decisions That Directly Affect an Individual.....	5
4.3 Records Retention and Disposal.....	5

PART 5:	FURTHER INFORMATION	5
5.1	Systematic Disclosures of Personal Information	5
5.2	Access for Research or Statistical Purposes	5
5.3	Other Applicable Legislation and Regulations.....	5
PART 6:	ACCESS AND PRIVACY MANAGER COMMENTS	6
6.1	Information or Materials Reviewed	6
6.2	Analysis and Findings	6
6.3	Conditions of Approval	6
6.4	Review and Distribution	6

TABLE OF FIGURES

Figure 1 - Major Document Revision Approval History	i
Figure 2 - Document Revision History and Revision Summary	i
Figure 3 - Major Document Revision Approval History	i
Figure 4 - Risk Mitigation Table.....	4

PART 1: GENERAL INFORMATION & OVERVIEW

1.1 Executive Summary

REDCap (Research Electronic Data Capture) is a web-based, metadata-driven EDC software solution and workflow methodology for designing and capturing data for research studies. REDCap allows users to build and manage online surveys and research databases quickly and securely. Use cases at UBC are varied, and will predominantly consist of projects that have received approval from UBC's Research Ethics Board (REB). REB-approved research projects are typically not subject to the PIA process. In some instances, REDCap may also be used for Quality Improvement/Quality Assurance (QI/QA) projects, subject to UBC's Data Access Request process and other project-specific conditions.

At UBC, REDCap is to be implemented by a variety of units, including the Centre for Teaching and Learning (CTLT), the Faculty of Medicine, Population Data BC, Psychology Department, and Advanced Research Computing (ARC). Each implementation of REDCap at UBC will follow Standard Operating Procedures (SOPs) determined by the responsible unit.

The PIA has identified key risks and mitigations in relation to administrative security controls, technical security controls, and information security design controls. Based on the information provided and mitigations in place, our review has concluded there are no significant unmitigated privacy or information security risks introduced by this project, however we do recommend the project ensure that it fully complies with the FIPPA legislation and the UBC Information Security Standards.

1.2 Description of the Program, System, Application, or Initiative Assessed

The following project description is applicable to UBC FoM use of REDCap only:

The MedIT Data Management team has been granted a license to use REDCap for the collection and storage of clinical research data. REDCap is a web-based software program created by Vanderbilt University and supported by the REDCap Consortium to facilitate clinical research and data collection. REDCap is also Health Insurance Portability and Accountability Act (HIPAA)–compliant, highly secure and intuitive to use. The databases use instruments such as surveys and forms as research capture tools. Projects are self-sufficient and secure databases that can be used for normal data entry or for surveys across multiple distinct time points. They are workflow-based and focus on collecting data and exporting it to statistical programs and other data analysis software. REDCap is designed to provide a secure environment so that research teams can collect and store highly sensitive information.

The MedIT Data Management team is responsible for administering the use of the software, including establishing policies for appropriate use of REDCap, providing access to users/databases, assuring regular audits of system use and providing general user support. Each project must have a designated Project Administrator who will be responsible for administration of the specific project, including building and maintaining the database/project, facilitating role-based access for users, confirming appropriate oversight committee approvals (e.g. Research Ethics Board or BC Health Authority) are in place prior to any data entry and assuring the ongoing integrity of the project data in REDCap. The Project Administrator will work closely with the FoM Data Management team, who will consult and train research teams along with providing routine audits of projects.

RISK CLASSIFICATION

The inherent privacy risk classification level of this PIA submission is 4 - High. The residual risk classification level of this PIA submission at closure is 2 - Low.

1.3 Scope of PIA

The scope of this PIA is the implementation of REDCap for direct use by UBC staff and students who are authorized to use the product on behalf of UBC. Administrative, business improvement, operational, or non-REB approved projects, including Qi/QA projects, are not covered by this PIA and are subject to a separate review.

1.4 Related PIAs

Not applicable.

1.5 Elements of Information or Data

The personal information (PI) collected will vary depending on the initiative or project requirements (and may require additional PIA requests if not approved by the REB). Users do not interact directly with the software, it only acts as an information repository.

An example use case by the UBC Faculty of Medicine (FoM) for clinical trials and medical research related to COVID-19 collects the following PI:

- First Name - for e-consenting and in some cases patient tracking
- Last Name - for e-consenting and in some cases patient tracking
- Date of Birth - full or partial typically used to calculate age
- Email address - for e-consenting, sending surveys/alerts
- Postal code - often 3 digits only
- Personal Health Information - REB approved for research
- Personal Health Number - must be approved by REB or regulatory bodies

1.6 Storage or Access Outside of Canada (including back-ups and recovery)

Not applicable.

1.7 Data-Linking Initiative

This project is not considered a data-linking initiative as contemplated under s.(36) of FIPPA.

1.8 Is this a Common or Integrated Program or Activity?

This project is not considered a common or integrated program or activity as defined in Schedule 1 of FIPPA.

PART 2: PROTECTION OF PERSONAL INFORMATION

2.1 Personal Information Flow Diagram / Table

PI collected will vary depending on the initiative or project requirements.

Legal aspects round PI collection are addressed through the REB approval project and are not subject to further review as part of the PIA.

Projects that are not REB approved may be sanctioned with appropriate third party approval, in partnership with UBC (on a case-by-case basis).

2.2 Risk Mitigation Table

The following table outlines risk identified in relation to the project and recommended response plan.

Category: Security					
Risk	Ref#	Inherent Likelihood	Inherent Impact	Response	Residual Risk
Weak or absence of technical security controls	RK0020650	4 - High	4 - Major	Mitigate	2 - Low
	Mitigation Plan: The project to conduct regular system monitoring will ensure that the research data and PI contained within the software is adequately secured from cyberattacks. Departmental Instance of REDCap is currently protected by traditional firewall, UBC Web Application Firewall (WAF) is recommended for further enhancement of security. The UBC FoM and UBC IT Cybersecurity teams are in agreement for implementing this change at a mutually convenient time.				
Weak or absence of information security design controls	RK0020649	4 - High	4 - Major	Mitigate	2 - Low
	Mitigation Plan: The project to engage with UBC Cybersecurity team to review the REDCap security posture, identify gaps and provide recommendations. In the case of the UBC FoM REDCap instance, the requirement to meet Health Canada and FDA platform validation for clinical trial/clinical research and to store health information is required to be in place.(This requirement has been met)				
Weak or absence of administrative security controls	RK0020651	4 - High	4 - Major	Mitigate	2 - Low
	Mitigation Plan: The project to implement administrative controls in line with UBC Information Security Standards to ensure only authorized users have access to REDCap, including use of UBC campus wide-login (CWL) and strong passwords, privileged account management, and enforcement of the 'least privilege' access controls. In addition, security validation testing and system-level monitoring and system/user activity logging are required to be in place.(This requirement has been met)				

Figure 4 - Risk Mitigation Table

2.3 Collection Notice

Persons having their PI collected and stored within REDCap are required to consent, the procedures to be outlined as part of the REB approval.

2.4 Consent for Storage/Access Outside of Canada & Opt-Out Procedure (If Any)

Not applicable. PI will be stored within Canada.

2.5 Consent Withheld Procedure

Not applicable. Consent is not required.

PART 3: SECURITY OF PERSONAL INFORMATION

3.1 Physical Security Measures

This project is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBC ISS (Information Security Standards).

3.2 Technical Security Measures

This project is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBC ISS (Information Security Standards).

3.3 Security Policies, Procedures, and Standards

This project is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBC ISS (Information Security Standards).

3.4 Tracking Access / Access Controls

Controlling access to REDCap is the responsibility of each unit. In line with UBC Information Security Standards and the 'least privilege' principle, administrator-level access will typically be limited to fewer than five people within each business unit. Access to personal information contained within REDCap is project dependent, and will be similarly limited (usually a principal investigator and project team).

PART 4: ACCURACY, CORRECTION, AND RETENTION

4.1 Updating and Correcting Personal Information

Not applicable.

4.2 Decisions That Directly Affect an Individual

This project does not capture personal information that directly affects an individual.

4.3 Records Retention and Disposal

This project is required to comply with UBC Records Management Policies.

PART 5: FURTHER INFORMATION

5.1 Systematic Disclosures of Personal Information

This project does not involve the systemic disclosure of personal information.

5.2 Access for Research or Statistical Purposes

This project does not involve the disclosure of personal information for research or statistical purposes as contemplated under s.(35) of FIPPA.

5.3 Other Applicable Legislation and Regulations

This project is not subject to other applicable legislation or regulations

PART 6: ACCESS AND PRIVACY MANAGER COMMENTS

6.1 Information or Materials Reviewed

Overall provided information was deemed reasonable to provide an understanding of operating privacy and security controls.

Information Reviewed	Date Received
BREB_ChecklistForResearchRequiringEthicsReview.pdf	2021-04-07 03:27:09
EA Security Brief-RedCap-v8 0 - signed oga.pdf	2021-04-08 02:36:41
Faculty of Medicine Research REDCap SOPS List.pdf	2021-04-21 02:52:23
FoM REDCap Installation Qualification.docx	2021-04-08 02:36:10
FoM REDCap Validation Certificate.pdf	2021-04-08 02:36:55
PS-REDCap-PrivacyStatement.pdf	2020-11-10 01:14:50
RedCAP_SecurityReview_Ver_2_0_April-19-2021.xlsx	2021-04-21 02:52:22
SS-REDCap-SecurityStatement.pdf	2020-11-10 01:14:50

6.2 Analysis and Findings

The information provided for the review has established that REDCap can be used in the proposed manner in compliance with FIPPA and UBC's Information Security Standards.

The following are the key factors in that determination:

- Personal information is collected, stored, and accessed within Canada;
- Personal information is not disclosed to third parties;
- Personal information is kept secure during transmission and at rest;
- Access requires use of a valid login credentials with appropriate access authorities.

This PIA also relied on conclusions of the UBC IT Cybersecurity review to establish that REDCap implementation at the Faculty of Medicine meets UBC security standards and has attained adequate level of controls. The review covered both administrative and technical controls, including reviewing documented procedures to manage safe and secure operations and a review of the servers and system security design and implementation. A detailed list of the reviewed artifacts is appended to this PIA.

Accordingly, REDCap can be used as proposed, subject to any conditions outlined in the following section.

6.3 Conditions of Approval

None specified.

6.4 Review and Distribution

This refers to the report approval process. The Owner is accepting the accuracy of the data provided to PrISM for this review and the risk responses. The Owner is responsible for the on-going operational activities and must ensure that this project continues to meet legislative and legal requirements, along with Information Systems Policy (SC14) requirements. Any change in PI collection or use will require new PIA.

Assessment Acceptance
Gurm Dhugga

This refers to the report distribution, including Requestor, Project Manager, Owner, and assigned Risk Advisor.

Distributed To

Requestor: Ashley McKerrow, Team Lead, Data Management
Project Manager: Ashley McKerrow, Team Lead, Data Management
Owner: Gurm Dhugga, Associate Director, Research & Digital Technology
Risk Advisor: Christian Stockman, Information Security Risk Advisor

PIA Request History:

PIA Request Date	Report Created
2020-10-16 15:20:29	2021-04-20 21:05:10