PIA01956 – UBC ARC REDCap

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	2021.07.15	Stockman, Christian	Report Creation

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

TABLE OF FIGURES

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 that have been externally approved in collaboration with clinical and BC Health Authority partners.

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

REDCap is a Research Data Capture tool. ARC provides two instances of REDCap hosted within EDUCloud for the UBC research community. Details of the system are provided on the ARC public web site http://arc.ubc.ca/standards including the platform architecture, privacy and security statements, terms of service, and security standards. The projects that may used the system are varied and will usually involve a variety of different data classifications, may or may not involve third parties, and other tools for storage and analysis within the project workflow. The only PI collected or processed by the tool would be as part of the research project and under the responsibility of the project owner as specified in the terms of service.

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 faculty, staff, students, researchers, external collaborators, and research participants who are authorized to use the product on behalf of UBC. Administrative, business improvement, operational, and non-REB approved projects are not covered by this PIA and may be subject to a separate PIA.

1.4 Related PIAs

Reference	Description
PIA01829	UBC REDCap Application

1.5 Elements of Information or Data

REDCap is a general research data capture tool. 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 generally do not interact directly with the software, it only acts as an information repository.

Data elements could be almost anything conceivable as PI, including but not limited to name, date of birth, address, contact information (e.g. address, telephone, email address), personal health number and other identifiers or information.

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

Not applicable.

1.7 Data-Linking Initiative

In FIPPA, "data linking" and "data-linking initiative" are strictly defined; if a project is a data linking initiative, it must comply with specific requirements under the Act related to data-linking initiatives.

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?

In FIPPA, "common or integrated program or activity" is strictly defined; where one exists it must comply with requirements under the Act for common or integrated programs and activities.

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: Privacy					
Risk	**Ref#**	**Inherent Likelihood**	**Inherent Impact**	**Response**	**Residual Risk**
Over collection of personal information	RK0020571	4 - High	4 - Major	Mitigate	2 - Low
	Mitigation Plan: PI collected is dependent on the specific project in question, and will vary. Legal aspects round PI collection will be addressed by REB approval and 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). (This risk has been mitigated)				
Category: Security					
Risk	**Ref#**	**Inherent Likelihood**	**Inherent Impact**	**Response**	**Residual Risk**
Weak or absence of technical security controls	RK0020724	4 - High	4 - Major	Mitigate	2 - Low
	Mitigation Plan: The project currently conducts regular system monitoring to ensure that the research data and PI contained within the software is adequately secured from cyberattacks. Regular system monitoring: This includes centralized logging, traditional internal and external web application vulnerability (credentialed and non-credentialed) scans, and manual threat intelligence. A vulnerability scanner will be implemented in 2021. Web Application Firewall: The ARC Instance of REDCap is currently protected by traditional firewall, UBC Web Application Firewall (WAF) is recommended for further enhancement of security. (This risk has been mitigated)				
Weak or absence of administrative security controls	RK0020573	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 risk has been mitigated)				

Figure 4 - Risk Mitigation Table

2.3 Collection Notice

If your initiative is collecting personal information directly from individuals then all individuals involved are informed of the following:

1. The purpose for which the personal information is being collected

2. The legal authority for collecting personal information, and

3. The title, business address and business telephone number of an officer or employee who can answer questions about the collection.

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

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

Consent is not required as use of REDcap will not result in the storage of personal information outside 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. The following documents have been reviewed as part of this PIA:

Information Reviewed	Date Received
BREB_ChecklistForResearchRequiringEthicsReview.pdf	2021-05-28 23:15:42
EA Security Brief-RedCap-v8 0 - signed oga.pdf	2021-05-28 23:15:43
PS-REDCap-PrivacyStatement.pdf	2021-05-28 23:15:43
RedCAP_SecurityReview_Ver_2_0_April-19-2021.xlsx	2021-05-28 23:15:43
SS-REDCap-SecurityStatement.pdf	2021-05-28 23:15:43

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 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.

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
Edith Domingue

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

Distributed To
Requestor: Scott Baker, Manager, Sensitive Research **Project Manager:** Scott Baker, Manager, Sensitive Research **Owner:** Edith Domingue, Manager, Research Platforms **Risk Advisor:** Christian Stockman, Information Security Risk Advisor

PIA Request History:

PIA Request Date	Report Created
2021-02-16 15:21:50	2021-07-15 19:37:18