PIA01894 – FoM OpenSpecimen

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	2021.07.07	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

OpenSpecimen is an open-source biobank laboratory information management system (LIMS) for tracking biospecimens from collection to utilization for research studies. the so ware allows users to collect data about biological research specimens, track specimen attributes, keep physical inventories and report findings. At UBC, OpenSpecimen is to be implemented primarily by the Faculty of Medicine (FoM) and maintained by the Medicine IT (MedIT) unit, following Standard Operating Procedures (SOPs) developed by that unit. 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, OpenSpecimen may also be used for tracking data as part of Quality Improvement/Quality Assurance (QI/QA) projects that have been externally approved in collaboration with clinical and BC Health Authority partners. Some projects may also be subject to UBC's Data Access Request process and other project-specific conditions.

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 FoM IT Data Management Team has procured an enterprise license to use OpenSpecimen to provide a platform for Biobanking. OpenSpecimen is designed to track biospecimens from collection to utilization for any type of collection. It achieves this by creating collection protocols of data based on your research needs (like smoking history, breast pathology annotations, genetics, lab tests, etc.) and use our powerful reporting module to get data out. OpenSpecimen integrates with other databases or instruments like REDCap, Epic, Oncore, Hamilton BiOS, etc.

In addition OpenSpecimen has an inventory management feature to allow users to physical organize their biobanks. For example, users can create any type of freezer with a configurable hierarchy and move boxes individually or in bulk. There is also a specimen distribution feature to allow users to manage and distribute specimens to researchers. It allows users to track requests and create invoices.

The FoM IT Data Management team is responsible for administering the use of the so ware, including establishing policies for appropriate use of OpenSpecimen, 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 (i.e., Research Ethics Board (REB)) are in place prior to any data entry and assuring the ongoing integrity of the project data in OpenSpecimen=. This Project Administrator will work closely with the FoM Data Management team, who will consult and train research teams along with providing routing 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 OpenSpecimen 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 review.

1.4 Related PIAs

Reference	Description
PIA01829	UBC REDCap Application
PIA01824	FoM Oracle Application Express Platform

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 typically do not interact directly with the software, it only acts as an information repository.

An example project for FoM clinical trials and medical research may collect the following PI:

- First Name
- Last Name
- Date of Birth
- Email Address
- Postal Code
- 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

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: Security					
Risk	**Ref#**	**Inherent Likelihood**	**Inherent Impact**	**Response**	**Residual Risk**
Weak or absence of technical security controls	RK0020765	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 so ware is adequately secured from cyberattacks. OpenSpecimen is currently protected by traditional firewall, UBC Web Application Firewall (WAF) is recommended for further enhancement of security. UBC FoM and UBC Cybersecurity team are in agreement for implementing this change at a mutually convenient time.				
Weak or absence of administrative security controls	RK0020767	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 OpenSpecimen, 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)				
Weak or absence of information security design controls	RK0020766	4 - High	4 - Major	Mitigate	2 - Low
	Mitigation Plan: The project to engage with UBC Cybersecurity team to review the OpenSpecimen security posture, identify gaps and and provide recommendations. The requirement for the UBC FoM 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)				

Figure 4 - Risk Mitigation Table

2.3 Collection Notice

Persons having their PI collected and stored within OpenSpecimen 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)

Consent is not required as use of OpenSpecimen 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).

OpenSpecimen uses AngularJS, a JavaScript framework which is reaching end of life for support in December 2021, potentially making OpenSpecimen vulnerable to future security issues. The vendor is aware of the end of life support and is working to replace AngularJS.

3.4 Tracking Access / Access Controls

Controlling access to OpenSpecimen is the responsibility of the FoM (specifically MedIT). 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 OpenSpecimen 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
FoM OpenSpecimen Installation Qualification.pdf	2021-07-01 06:46:29
OpenSpecimen screenshots.docx	2021-07-01 06:46:29
OpenSpecimen_SecurityReview_v2.0_June21.xlsx	2021-07-01 06:42:17
PIA20051-OpenSpecimen - 2020-12-18_FINAL.pdf	2021-03-09 05:37:42
Research DM SOP 205 OpenSpecimen User Accounts.docx	2021-07-01 06:46:29
Research DM SOP 210 OpenSpecimen Bug Management.docx	2021-07-01 06:46:29
Research DM SOP 215 OpenSpecimen Software Upgrade.docx	2021-07-01 06:46:29

6.2 Analysis and Findings

The information provided for the review has established that OpenSpecimen 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 OpenSpecimen 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.

Accordingly, OpenSpecimen 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: Gurm Dhugga, Associate Director, Research & Digital Technology
Owner: Gurm Dhugga, Associate Director, Research & Digital Technology
Risk Advisor: Christian Stockman, Information Security Risk Advisor

PIA Request History:

PIA Request Date	Report Created
2021-01-05 18:12:21	2021-07-07 10:32:36