PIA02309 — Wellspring Sophia

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
Taylor Bohn	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	2023-06-23	Taylor Bohn	Report Creation

Figure 2 - Document Revision History and Revision Summary

TEMPLATE REVISION APPROVAL

REVISION #	DATE	REVISED BY	DESCRIPTION
1.00	2023-06-23	William Sharp	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

The UBC University-Industry Liaison Office (UILO) is responsible for managing contracts, relationships and patents associated with UBC. UILO will be moving the existing repository to a new service, the Sophia Knowledge Management System, by Wellspring. Sophia is a cloud-based knowledge management application designed for small to large laboratories and facilities, enabling streamlining of the knowledge supply chain lifecycle, including capturing information on assets, inventions, and patents, as well as managing contracts as well as agreements.

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

The University-Industry Liaison Office (UILO) manages over 3000 contracts and agreements per year with a total value to the University of more than $200 million. To effectively manage these contracts and associated intellectual property (IP) assets on behalf of the university the UILO requires a sophisticated database capable of managing both IP/technology and agreements/contracts. We have selected the Wellspring Sophia software to replace our current system.

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 **3 - Low**.

1.3 Scope

Collection of personal information by authorized UBC administrators using Wellspring application, as outlined in this PIA.

1.4 Data Elements

The system will capture the names and contact details (addresses, personal phone numbers) of researchers (both Faculty and Students) at UBC who have submitted invention disclosures. In many cases citizenship data will also be captured (necessary for patent applications). It will further capture information about payments made to those researchers.

Personal information is captured primarily for the following reasons (a) to confirm the identify of inventors on patents, (b) to ensure that we can distribute revenue to inventors per UBC Policy LR11, and (c) to provide required information to national patent offices.

Researchers are required to provide their names and contact details (i) when completing invention disclosures, and (ii) when completing revenue sharing agreements.

UBC Finance (accounts payable) will give PI to researchers to process revenue sharing benefits. National Patent Offices require certain researchers PI (names, home addresses, citizenship) to file patents in UBC's name.

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

Personal information will be securely stored on AWS servers within Canada, with backup on Google Cloud Platform, as outlined in the diagram below.

1.6 Data-Linking Initiative

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

1.7 Is this a Common or Integrated Program or Activity?

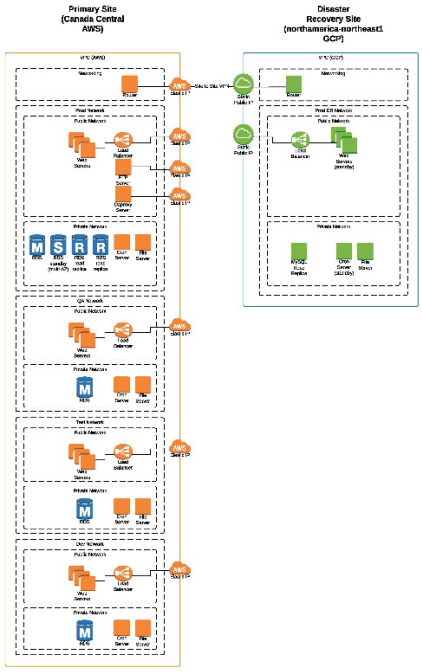
This project is not considered a common or integrated program or activity as defined in Schedule 1 of FIPPA.

PART 2: PROTECTION OF PERSONAL INFORMATION

2.1 Personal Information Flow Diagram / Table

Users will log-in to the Sophia system via Single Sign-On using UBC CWL. Wellspring will integrate with UBC's SSO/SAML system to ensure user authentication.

The following data flow diagram has been provided in support of this PIA, outlining the data storage and backup locations:



The following list of sub-processors has been identified:

- AWS – Cloud Hosting Service - Central Canada AWS (Primary) and Montreal (DR).
- Zendesk – Help Center / Sub-processor of certain end-user data (name, email).
- Google Gmail – Internal email Communication Tool / May contain end-user names and emails.
- Basecamp – Project Collaboration Software / May contain end-user names and emails.
- Sisense – Business Intelligence Tool / May be used to support dashboards with names.

The vendor has confirmed no personal information is shared with third parties by Wellspring.

2.2 Risk Mitigation Table

The following table indicates the associated risk levels as applicable and the potential or intended mitigation steps.

Category: Security					
Risk	**Ref#**	**Inherent Likelihood**	**Inherent Impact**	**Response**	**Residual Risk**
Retaining PI longer than necessary	RK0021438	4 - High	3 - Significant	Mitigate	3 - Medium
	Mitigation Plan: A data retention plan has not been submitted by the project. The unit is recommended to work with UBC Records Management to develop detailed retention schedules, particularly given the sensitivity of the data elements and research data to be collected within the service.				
Inadequate third party information sharing controls	RK0021446	4 – High	4 – Major	Mitigate	3 - Medium
	Mitigation Plan: No personal information is shared with third parties by Wellspring. There is some required information sharing within UBC between units, including financial and revenue sharing agreements, citizenship, and taxation information. This is required for regulatory and compliance purposes.				
Disposing of personal information using inadequate methods	RK0021572	4 - High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: The project is recommended to develop a detailed disposal plan, outlining how data will be migrated from the legacy system and what will happen to the legacy data/system once this process is complete.				
Over-collection of personal information	RK0021125	4 – High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: Personal information collected is required for the purposes of managing the relationship between the University and innovation/patent holders. The project is recommended to collect the minimum required personal information, as outlined within the Data Elements section, and to avoid collecting SIN number or financial information (deemed Very High Risk, per Security Classification of UBC Electronic Information -- Information Security Standard U1). This data should be obtained from other UBC databases which should remain the sole repository of such information, such as Workday. The project has agreed to limit collection to the data required, and to avoid collecting SIN within Sophia. This will be collected and retained locally on an encrypted spreadsheet, as this data is required as part of the invention disclosure and for UBC Accounts Payable to ensure licensing revenue and correct tax slips are created. Other personal information data elements are required as part of the invention disclosure process.				
Category: Security					
Risk	**Ref#**	**Inherent Likelihood**	**Inherent Impact**	**Response**	**Residual Risk**
Weak or absence of technical security controls	RK0021574	4 – High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: The vendor has provided security attestations in the form of ICO 27001 certification as well as a completed HECVAT. These documents outline key controls that are in place to mitigate privacy and security risks. The information contained in the HECVAT suggests that the vendor is heavily reliant on the AWS hosting platform for security controls. However, the vendor's own documentation and internal processes suggest that they strive to align to internationally recognized frameworks and standards (e.g., ISO, NIST). Per the HECVAT, the controls that are stated to have been put in place are acceptable for use at UBC.				
Use of third-party applications with inadequate controls	RK0021439	4 - High	3 - Significant	Mitigate	3 - Medium
	Mitigation Plan: As the vendor has not completed a third-party attestation, it is recommended the project monitor security closely, and continue to work with the vendor to ensure adequate controls are in place, in alignment with the UBC Information Security Standards. It is also recommended that the service implement a Web Application Firewall to enhance protection of the data hosted within the AWS infrastructure.				

Figure 4 - Risk Mitigation Table

2.3 Collection Notice

A standard UBC collection notice is required to be implemented when personal information is collected. A sample follows:

Your personal information is collected under the authority of section 26(c) of the Freedom of Information and Protection of Privacy Act (FIPPA). This information will be used to manage your relationship with UBC in the context of invention and patent disclosures. Questions about the collection of this information may be directed to XXXXX@ubc.ca.

It is advised that the FIPPA-required privacy notification be presented to the individual when they submit their invention disclosure, or when they register and provide their personal information.

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

Not required.

2.5 Consent Withheld Procedure

Not applicable.

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).

UBC has had limited visibility into or access to Wellspring's own information security policies, practices, or standards. Publicly available information, as well as detailed provided by the vendor, including a HECVAT report, asserts that Wellspring employs acceptable standards and practices in line with global standards and frameworks; however, these assertions could not be substantiated as no third-party attestation has been completed. This has been noted in the risks table.

3.4 Tracking Access / Access Controls

Access should be granted to individuals on a need to know basis only. Users will have access to the system to submit invention disclosures and contract requests. They can also log in to see information related to their own submissions. Only UBC UILO staff will have access to full data. At UBC, this is a permission defined by the organization. In general, this is limited to UILO staff. At Wellspring, Operations and Engineering have access to personal information, and this is limited to: name, address phone and e-mail.

PART 4: ACCURACY, CORRECTION, AND RETENTION

4.1 Updating and Correcting Personal Information

Personal information may be updated by individuals whose personal information has been collected contacting the UILO, as required.

4.2 Decisions That Directly Affect an Individual

This project captures personal information that directly affects an individual and would be required to be retained for at least one year under s.(31) of FIPPA.

4.3 Records Retention and Disposal

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

The project has not developed a defined records retention plan and is encouraged to do so. The vendor has noted that data retention procedures are dependent on data type and can be changed based on client requirements. This has been noted in the risks table.

PART 5: FURTHER INFORMATION

5.1 Systematic Disclosures of Personal Information

This project does not involve the systemic disclosure of personal information. However, some data elements are shared with other UBC units (e.g., Finance) to enable payments.

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

Information Reviewed	Date Received
HECVAT302_Full_Sophia.xlsx	2023-06-02 21:16:45
ISO 27001 Controls List.xlsx - ISO Control Domains.pdf	2023-06-02 21:22:12
RE_ Comment added to_ Wellspring Sophia - Technology Management System (#INC2749520).msg	2023-06-02 21:16:45
Security Statement_Template_Sophia_2021.docx.pdf	2023-06-02 21:22:12
SOC 2 - AWS SOC 2 Report 2021 FINAL.pdf	2023-06-02 21:22:14
SOC_Continued_Operations_Letter.pdf	2023-06-02 21:22:13
Sophia Diagram (AWS CA) (1).jpg	2023-06-02 21:17:54
Sophia Diagram (AWS CA) (1).pdf	2023-06-02 21:16:44
Sophia Diagram (AWS CA).pdf	2023-06-02 21:22:11
UBC_MLSA_WW_V4-Clean.pdf	2023-06-02 21:22:14
Wellspring Worldwide - ISO 27001 Certificate - 2022.pdf	2023-06-02 21:16:45
Wellspring Worldwide Incorporated ISO 27001 Certificate-with signature-1-2-1.pdf	2023-06-02 21:22:13

6.2 Analysis and Findings

Based on the information provided, our review has concluded there are no significant privacy or security risks introduced by this project or use-case. The project may proceed in the proposed manner as long as it continues to fully comply with the FIPPA legislation and the UBC Information Security Standards, subject to the conditions of approval in the next 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
John-Paul Heale

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

Distributed To
Requestor: William Sharp, Associate Director, Technology Transfer **Project Manager:** William Sharp, Associate Director, Technology Transfer **Owner:** Mark John-Paul Heale, Managing Director, University Industry Liaison **Risk Advisor:** Christian Stockman, Senior Advisor, Privacy and Information Security Risk

PIA Request History:

PIA Request Date	Report Created
2022-04-04 10:47:03	2023-06-02 16:14:37