PIA01824 – FoM Oracle Application Express Platform

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	2021.09.21	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

Oracle Application Express (APEX) is a low-code development platform for building data applications (apps). Using APEX, data teams can develop and deploy apps to support research projects. Features of the platform include: Enables IT team to rapidly create data applications from concept to working prototype, build secure web-based relational apps which are mobile-ready, support machine learning and analytics (R) frameworks and enables integration with other data assets with API capabilities.

At UBC, Oracle APEX 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 FoM 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, may also be used for Quality Improvement/Quality Assurance (QI/QA) projects and unit level administrative projects 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 following project description is applicable to UBC FoM use of Oracle APEX only:

Under UBC Enterprise Oracle site license, FoM Data Management team has acquired a license to use Oracle APEX. Oracle APEX is a commercial so ware that can be used to create data applications to support collection, storage and integration of data.

Use case: BC COVID-19 Consent to Contact Research Registry
In collaboration with the BC Centre for Disease Control (BCCDC), UBC FoM has developed and will maintain a registry of patients who have recovered or are recovering from COVID-19 and have consented to be contacted about research initiatives related to COVID-19. The purpose of the Consent Registry is to support research that may assist in improving care for those who have been infected with COVID-19 and to discover strategies for controlling the epidemic in the future. The Initiative was submitted to and has received approval from the UBC Clinical REB, Provincial Health Services Authority and BC's Office of the Information and Privacy Commissioner.

The MedIT Data Management team is responsible for administering the use of the so ware, including establishing policies for appropriate use of Oracle BCCDC, 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, facilitating role-based access for users, confirming appropriate oversight committee approvals (e.g. REB or BC Health Authority) are in place prior to any data entry and assuring the ongoing integrity of the project data in Oracle APEX. 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 limited to the implementation of Oracle APEX at FoM, 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. The scope of the PIA is further limited to data applications developed by FoM MedIT personnel in compliance with the UBC IT Security standards. The use of FoM Oracle platform for application development by non-MedIT personnel may be subject to a separate review

1.4 Related PIAs

Reference	Description
PIA01829	UBC REDCap Application
PIA01894	FoM OpenSpecimen

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 so ware, it only acts as an information repository.

As outlined above an example use case by the UBC Faculty of Medicine (FoM) is the BC COVID-19 consent to contact registry which collects the following PI:

- Provincial Health Number (PHN): for purposes of linking health data
- Name: for consenting and in some cases patient tracking
- Age: for inclusion/exclusion criteria of studies
- Date of Birth: Calculate Age
- Sex: for specific Covid-19 cohort studies
- Mailing Address: for consenting and contact
- Email Address: for consenting and contact
- Telephone number: for consenting and contact
- Regional Health Authority (RHA): for inclusion/exclusion criteria of studies
- Date of Symptom Onset: for specific Covid-19 cohort studies
- Hospitalization (optional):
- Resident of Long-Term Care Facility or Correctional Facility (Yes/No): for inclusion/exclusion criteria of studies
- Pregnancy: for inclusion/exclusion criteria of studies
- Survival Status: for inclusion/exclusion criteria of studies

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

The Oracle APEX platform itself does not collect any personal information.

PI hosted on the platform will vary depending on the initiative or project requirements.

Legal aspects around 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	RK0020901	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. Oracle APEX 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 information security design controls	RK0020903	4 - High	4 - Major	Mitigate	2 - Low
	Mitigation Plan: The project to engage with UBC Cybersecurity team to review the Oracle APEX security posture, identify gaps 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)				
Weak or absence of administrative security controls	RK0020902	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 Oracle APEX, 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

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 Oracle APEX 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 Oracle APEX 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

For example: locked cabinets, securely stored laptops, or key card access to the building.

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 Oracle APEX 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 Oracle APEX 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

This section indicates reference materials which were provided to support this review.

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_OracleApex_PIAScopeDRAFT.docx	2021-09-21 02:30:25
FoM_OracleApex_SecurityReview_v1.0.xlsx	2021-09-21 02:30:25
How to Achieve GDPR Compliance with Oracle APEX - Spire Software.pdf	2020-11-03 21:25:25
Oracle APEX Security.pdf	2020-11-03 21:25:27
Oracle APEX Services Privacy Policy.pdf	2020-11-03 21:25:27

6.2 Analysis and Findings

This is the assessment based on the project materials provided for review.

The information provided for the review has established that Oracle APEX can be used in the proposed manner incompliance 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.

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

This PIA also relied on conclusions of the UBC IT Cybersecurity review to establish that Oracle APEX implementation at the FoM 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.

6.3 Conditions of Approval

Where applicable, this refers to any conditions or limits to the scope for this PIA.

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
2020-10-09 22:04:40	2021-09-21 19:00:39