PIA02164 — Knebel Knotes

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	
Christian Stockman	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	2021-10-28	Christian Stockman	Report Creation

Figure 2 - Document Revision History and Revision Summary

TEMPLATE REVISION APPROVAL

REVISION #	DATE	REVISED BY	DESCRIPTION
1.00	2021-10-28	Ryan Knebel	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 Department of Psychiatry will use Knebel Knotes, a mobile app reference tool developed by a clinical psychiatry faculty member that allows users to look up prescription drug information quickly and easily. This app is not required for a particular class and will exist primarily as a reference for students who wish to download it. The app was developed on the Firebase platform (Google), used for creating mobile and web applications for the Android and Apple web stores. No personal information is accessed or shared by the app. however Firebase will collect personal information from users (see Data Elements section of this PIA). Although the app does not collect any personal information, payment for annual app subscription is collected via the app stores. In addition, the app's developer/administrator will have access to user IDs and email addresses for the purposes of managing paid subscriptions. UBC does not require any personal information to be collected from app users.

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

Knebel Knotes app provides a quick reference for prescribing most psychiatric medications. It focuses on key information each medication is known for, to help support clinical practice and facilitate learning. The information provided is NOT meant to serve as a comprehensive drug monograph, but instead highlights key information for the learning of a clerkship student or junior resident.

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

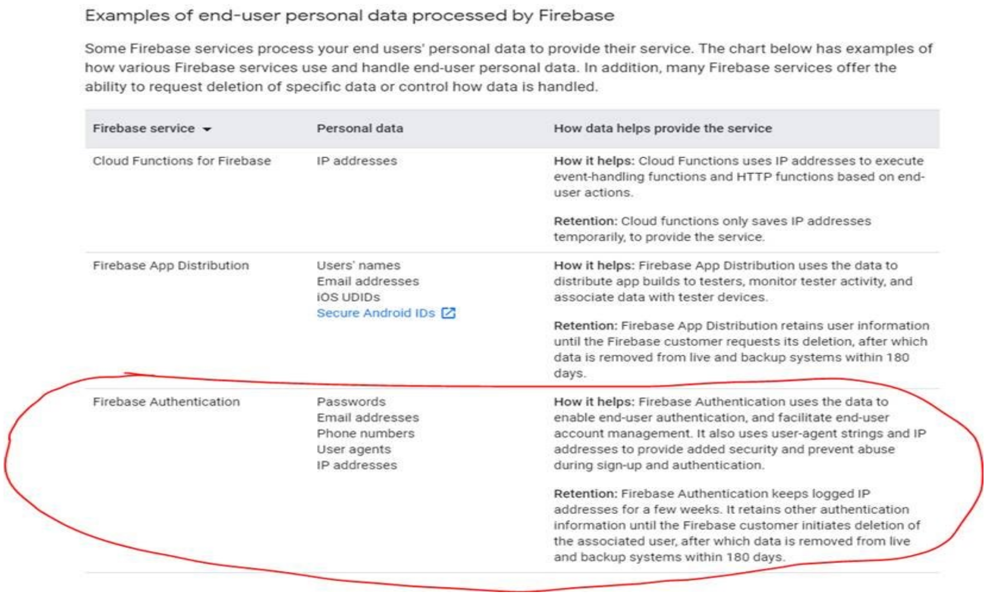
The scope of this PIA is the implementation of Knebel Knotes mobile app for direct use by UBC users, including faculty, staff and student who are authorized to use the product, as outlined in this PIA.

1.4 Elements of Information or Data

Personal information is collected by the by the Android and/or Apple app stores and by the Firebase mobile application development platform (all out of scope for this PIA).

Personal information accessed by the app developer for the purposes of managing paid registrations includes AppleID or AndroidID and email address, accessed via the Firebase platform.

The Firebase platform collects personal information (via the app stores), as outlined below, as part of users' interactions with the app stores:



Examples of end-user personal data processed by Firebase

Some Firebase services process your end users' personal data to provide their service. The chart below has examples of how various Firebase services use and handle end-user personal data. In addition, many Firebase services offer the ability to request deletion of specific data or control how data is handled.

Firebase service ▾	Personal data	How data helps provide the service
Cloud Functions for Firebase	IP addresses	**How it helps:** Cloud Functions uses IP addresses to execute event-handling functions and HTTP functions based on end-user actions. **Retention:** Cloud functions only saves IP addresses temporarily, to provide the service.
Firebase App Distribution	Users' names Email addresses iOS UDIDs Secure Android IDs	**How it helps:** Firebase App Distribution uses the data to distribute app builds to testers, monitor tester activity, and associate data with tester devices. **Retention:** Firebase App Distribution retains user information until the Firebase customer requests its deletion, after which data is removed from live and backup systems within 180 days.
Firebase Authentication	Passwords Email addresses Phone numbers User agents IP addresses	**How it helps:** Firebase Authentication uses the data to enable end-user authentication, and facilitate end-user account management. It also uses user-agent strings and IP addresses to provide added security and prevent abuse during sign-up and authentication. **Retention:** Firebase Authentication keeps logged IP addresses for a few weeks. It retains other authentication information until the Firebase customer initiates deletion of the associated user, after which data is removed from live and backup systems within 180 days.

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

The app itself does not collect or store personal information, but the app stores and development platform does collect personal information.

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

No Applicable.

2.2 Risk Mitigation Table

Category: Security					
Risk	**Ref#**	**Inherent Likelihood**	**Inherent Impact**	**Response**	**Residual Risk**
PI stored / accessible outside of Canada	RK0020190	4 - High	4 - Major	Mitigate	2 - Low
	Mitigation Plan: The project to implement privacy and consent notification and obtain consent from a student prior their personal information is collected, used and disclosed outside of Canada. This includes storage location, and technical and operation supports from outside of Canada. A proposed consent notice is captured in the Recommended Collection Notice section of this PIA.				
Over collection of personal information	RK0020929	4 - High	4 - Major	Mitigate	2 - Low
	Mitigation Plan: Personal information collected is required by the app stores in order to have an account and to enable purchasing of apps. UBC does not collect or access personal information collected by the app stores, except as outlined in the Data Elements section.				
PI stored / accessible outside of Canada	RK0020921	4 - High	4 - Major	Mitigate	2 - Low
	Mitigation Plan: Personal information collected within the app stores and processed within the Firebase platform is done so independently and is not shared with UBC. No personal information is shared by the University.				

Figure 4 - Risk Mitigation Table

2.3 Collection Notice

The following is recommended to be added to the respective app stores to inform users:

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 for the purpose of downloading the using the Knebel Knotes app as a UBC student. By submitting your personal information, you are consenting to the storage of this information on a secure server located in the United States. Questions about the collection of this information may be directed to XXXXX@ubc.ca.

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

Consent is not required as use of [Insert Tool] will not result in the storage of personal information outside Canada.

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).

3.4 Tracking Access / Access Controls

The app developer/administrator will be able to access the list of subscribed users only, in order add and delete users manually. Only app store user IDs and email addresses are accessible for this purpose.

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

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

6.2 Analysis and Findings

The information provided for the review has established that Knebel Knotes and the associated use-case, as presented by the UBC Faculty of Medicine Department of Psychiatry, can be used in the proposed manner in compliance with FIPPA and UBC policies and standards.

The following are the key factors in that determination:

- Personal information is collected, stored, and accessed within Canada, and outside of Canada with appropriate consent;
- Personal information is not disclosed to third parties external to authorized UBC staff members;
- Information is kept secure during transmission and at rest.

Accordingly, Knebel Knotes can be used as proposed subject to the conditions outlines in the following section.

6.3 Conditions of Approval

Changes to the app such as collection of additional personal information, will require a new PIA
Confirmation of the proposed process by which the Department of Psychiatry will utilize the application for its students.

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
Ryan Knebel

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

Distributed To
Requestor: Ryan Knebel, Clinical Instructor **Project Manager:** Ryan Knebel, Clinical Instructor **Owner:** Ryan Knebel, Clinical Instructor **Risk Advisor:** Christian Stockman, Information Security Risk Advisor

PIA Request History:

PIA Request Date	Report Created
2021-09-24 14:17:05	2021-10-28 21:31:40