PIA02494 – Cortico Patient Booking Software

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	2023-06-27	Christian Stockman	Report Creation

Figure 2 - Document Revision History and Revision Summary

TEMPLATE REVISION APPROVAL

REVISION #	DATE	REVISED BY	DESCRIPTION
1.00	2023-06-27	Hope Akello	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

UBC Pharmaceutical Sciences will be implementing Cortico, a patient booking software that interacts with the existing OSCAR EMR already in use at UBC Pharmacy. Cortico is designed to streamline appointment booking and validation, and to allow for the transmission of documents between patients and the clinic. The service is designed with privacy by design principles in mind and does not store any personal or health information. Rather, it acts in a collection mechanism that interacts with OSCAR, which continues to be the system of record.

The service functions as an API client connected to OSCAR, to ensure that the correct information is transmitted to the patient's OSCAR profile. It also allows for telehealth calls between the doctors and patients, using the WebRTC videoconferencing functionality with encryption built into each web browser rather than a proprietary service. In addition, Cortico offers a concierge service to help clinics send mass emails. This involves handling and uploading patient email contact lists. These messages, as well as real-time messages are sent via a browser extension using Amazon SES (SMS and email) and Canadian messaging gateways. Finally, the service will allow for the secure transmission of documents between the patient and OSCAR, utilizing temporary Amazon S3 storage facilities within Canada.

The company is based in Burnaby, BC, with application servers in the same location (Cologix).

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

The UBC Pharmacists Clinic would like to explore a new appointment booking software and has selected Cortico (https://cortico.health/) as an option. The online appointment booking system currently used within the UBC Pharmacists Clinic is powered by Veribook.

Veribook is "an online scheduling service that integrates with OSCAR EMR to enable patients to self-book appointments and synchronize each booking with the Clinic's OSCAR scheduling templates." However, there are several limitations with this system:

- Patients must sign up and create a separate Veribook account in order to book an appointment at the Clinic.
- The MOA team cannot view the patient's email address. The MOA team must obtain patient demographic and appointment information prior to the appointment. This information is used to create a patient chart within the EMR system and to inform the clinician prior to the appointment. Since patient email addresses are not visible within Veribook, the MOA team must call every patient who has completed an online booking to confirm details and to obtain their email addresses to share an intake form.
- This can be annoying or frustrating for patients who are comfortable using technology and believed they successfully completed an online booking. Additionally, this becomes one more task for the MOA team to complete with each online booking.
- Veribook reminder emails cannot be manually pushed. Sometimes these emails are delayed or mistakenly deleted by patients and the MOA team has no way to easily re-send or edit the message.
- The copy within the confirmation emails (at time of booking) and the reminder emails (48hrs) cannot be different. Veribook does not allow differentiating.

Several patients have requested text message reminders, which is not possible with Veribook. For these reasons and due to the overall restrictive nature of Veribook, the UBC Pharmacists Clinic would like to transition to a new service to streamline patient to clinic communication and relieve administrative workload. The proposed new service is offered by Cortico and is designed to streamline appointment bookings and validation, while also allowing for the secure transmission of messages and documents between patients and clinics.

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

Use of Cortico software for appointment booking, validation and document submission, video communication, secure document and message sharing between by patients and users authorized to use the application in the context of their relationship with the University.

1.4 Data Elements

Cortico communicates with the clinic's OSCAR EMR system. Personal health information is collected and displayed but never stored within Cortico. This information includes:

- Personal Health Number
- Date of birth
- Email
- Sex (as stated on patient care card)
- Allergies
- Phone number
- Address
- Emergency contact information
- Reason for visit
- Medical conditions
- Medications
- Pronouns
- Health Care Team (names and contact information)

Personal information contained within the EMR may include name, age, date of birth, personal health number, contact information (email, phone number, address), health/medical information such as medical conditions, medical history, assistive devices, medications, and allergies.

Cortico's use of Amazon Web Services tools may allow AWS to retain personal information for audit and diagnostic purposes (e.g. telephone and email).

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

Personal information is stored on OSCAR EMR servers hosted securely at UBC.

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.

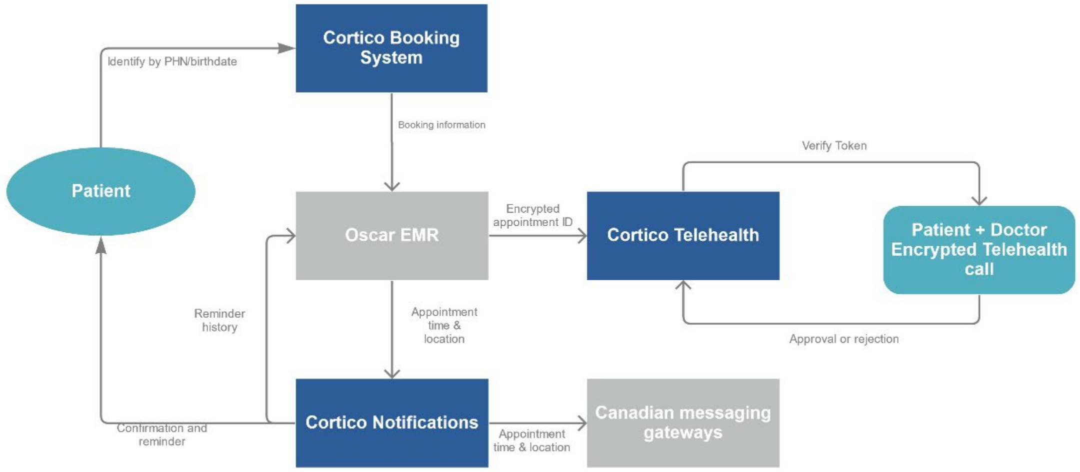
PART 2: PROTECTION OF PERSONAL INFORMATION

2.1 Personal Information Flow Diagram / Table

Per the vendor, the Cortico application is a front-end user interface application provided via the web and electronic device that collects PHI but never stores it. The PHI is forwarded via Cortico to an electronic medical records software application (OSCAR EMR) that then processes such information to handle scheduling, appointments, reminders, alerts, changes and other functions associated with patient booking. The EMR stores and administers the PHI and account information. The Program can also pull information from EMR and display it on a user interface to view but without storing that information on the Program. Due to the nature of the Program such PHI can never be accessed by Cortico personnel whether it is inputted on the Program user interface or viewed via that user interface.

Regarding messages and document transmissions, Amazon SES logs sent messages for a period of 30 days (not contents, but contact info) which is made available to Cortico DevOps staff for audit & troubleshooting. Documents may be sent one-way only from the patient, stored temporarily in an encrypted Amazon S3 bucket (within Canada). Documents will rest within OSCAR and may be downloaded from there using challenge questions and unique ID known to the patient, such as personal health number. The clinic may send either documents stored on the computer or documents stored within OSCAR. To send a document to a patient, that document can be emailed to a patient where it is received as a protected link. Patients may download or fill out the e-form after entering their personal health number and date of birth.

The following data flow was provided in support of this project:


Cortico Booking System
Identify by PHN/birthdate
Booking information
Patient
Oscar EMR
Encrypted appointment ID
Cortico Telehealth
Verify Token
Patient + Doctor Encrypted Telehealth call
Approval or rejection
Reminder history
Appointment time & location
Cortico Notifications
Confirmation and reminder
Appointment time & location
Canadian messaging gateways

2.2 Risk Mitigation Table

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

Category: Privacy					
Risk	**Ref#**	**Inherent Likelihood**	**Inherent Impact**	**Response**	**Residual Risk**
Over collection of personal information	RK0021334	4 - High	4 - Major	Mitigate	1 - Very Low
	Mitigation Plan: Personal information is not collected as part of this service. The service acts as a web form as pass data through to the OSCAR EMR system.				
Category: Security					
Risk	**Ref#**	**Inherent Likelihood**	**Inherent Impact**	**Response**	**Residual Risk**
Weak or absence of information security design controls	RK0021597	4 - High	4 - Major	Mitigate	2 - Low
	Mitigation Plan: Cortico is designed specifically to minimize access to personal information, while still allowing for the purposes of appointment scheduling and providing personal information to the OSCAR EMR, which will continue to serve as the system of record.				

Figure 4 - Risk Mitigation Table

2.3 Collection Notice

A standard collection notice must be provided at the time personal information is collected.

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).

3.4 Tracking Access / Access Controls

Cortico staff do not have access to personal information, with the exception of encrypted files stored on the server for transfer (and then only in limited circumstances). 5-6 staff at Cortico have troubleshooting capabilities providing broad technical access for this purpose (however not able to decrypt encrypted files or access personal information while in transit). The UBC contract will note specifics around security and confidentiality for Cortico staff who may have access for troubleshooting purposes.

PART 4: ACCURACY, CORRECTION, AND RETENTION

4.1 Updating and Correcting Personal Information

Users will use the service to provide personal information to be validated with the data already with OSCAR EMR. Personal information would be updated directly at the time of clinic appointment.

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

Information Reviewed	Date Received
Cortico Customer Services Agreement 220930.docx.pdf	2023-06-16 23:14:28
Cortico Customer Services Agreement 230405 (Hero).docx	2023-06-17 00:00:52
Cortico Data Flow Diagram.jpg	2023-06-16 23:14:29
Cortico Health Technologies Inc. HIPAA-.pdf	2023-06-17 00:00:52
Cortico Health Technologies ISO 27001 - 2687.pdf	2023-06-16 23:14:29
Cortico Privacy Policy.pdf	2023-06-17 00:10:04
HIPAA-Report Cortico Health Technologies Inc.pdf	2023-06-17 00:00:52
Patient Terms of Service and Privacy.docx	2023-06-16 23:14:28
Privacy-and-Information-Security-Requirements-and-Risk-Assessment-v1.2.xlsx - CORTICO.pdf	2023-04-22 01:13:18
Privacy-and-Information-Security-Requirements-and-Risk-Assessment-v1.2.xlsx - Questionnaire UBC.docx	2023-06-16 23:14:28
Privacy-and-Information-Security-Requirements-and-Risk-Assessment-v1.2.xlsx - Questionnaire.pdf	2023-06-16 23:14:28
UBC Privacy Requirement Items.docx	2023-06-16 23:14:28

6.2 Analysis and Findings

The information provided for the review has established that the project and associated use-case, as presented, can be used in the proposed manner. Based on the information provided, there are no significant privacy or information security risks introduced by this project. We do, however, recommend the project ensure that it continues to fully comply with the FIPPA legislation and the UBC Information Security Standards.

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
Barbara Gobis

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

Distributed To
Requestor: Hope Akello, Healthcare Designer **Project Manager:** Hope Akello, Healthcare Designer **Owner:** Barbara Gobis, Director, Pharmacists Clinic **Risk Advisor:** Christian Stockman, Senior Advisor, Privacy and Information Security Risk

PIA Request History:

PIA Request Date	Report Created
2022-11-03 10:45:17	2023-06-27 12:30:05