PIA02136 – COVID Tracking or Proof of Vaccination

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 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.

Contributors

CONTRIBUTOR	DEPARTMENT	POSITION
Tremonti, Robert	Safety and Risk Services	Lead Advisor, Privacy and Information Security Risk
Hancock, Paul	Office of the University Counsel	Legal Counsel, Information and Privacy
Lonsdale-Eccles, Michael	Safety & Risk Services	Director, Privacy & Information Security Management

PIA Major Version & History

VERSION	DATE ISSUED	ACTIVITY	REMARKS / MAJOR CONTENT & FUNCTIONALITY
1.0	2021-09-13	Assessment of vaccination declaration	Declaration of vaccination status
2.0	2021-10-08	Assessment of rapid testing and evidence of vaccination	▪ Upload proof of vaccination ▪ Ability to book appointments at testing clinic ▪ Reports and extracts to support new functionality ▪ Broadcast e-mails to students and employees ▪ Recording of rapid test results ▪ Reporting of positive tests to health authorities

TABLE OF CONTENTS

PART 1: GENERAL INFORMATION & OVERVIEW

1.1 Executive Summary

As part of the September 2021 safe return to campus, the University is requiring all faculty, staff, and students to complete a declaration regarding their COVID-19 vaccination status prior to returning to campus. This information will be used for the purpose of determining if participation in the COVID-19 rapid testing program is required.

This PIA considers all collection, use and disclosure of information associated with the vaccination declaration, evidence collection and testing.

This PIA will be delivered in versions, aligned with the program delivery phases.

Completed Program Delivery Phases

- The first project delivery phase included the platform supporting the process (Thrive Health), and a declaration of vaccination status.
- The second project delivery phase included processes for collection of proof of vaccination, scheduling of clinic appointments, issuing of broadcast e-mails to employee and students, recording of rapid test results, and reporting of positive test results to the respective local Health Authority. Based on the information provided and mitigations specified in this report, our review has concluded there are no significant unmitigated privacy or information security risks introduced by the second phase of this project which will not be resolved satisfactorily though the lifecycle of the program.
- Based on the information provided and mitigations specified in this report, our review has concluded there are no significant unmitigated privacy or information security risks introduced by the first and second phases of this project which will not be resolved satisfactorily though the lifecycle of the program.

Future Program Delivery Phases

- The third program delivery phase will include processes for validation of submitted proof of vaccination, audit and compliance processes, and associated reporting and retention processes. These processes have not been finalized, and will be considered in a future version of the PIA.

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

Program

As part of the September 2021 safe return to campus, the University is requiring all faculty, staff, and students to complete a declaration regarding their COVID-19 vaccination status prior to returning to campus. This information will be used for the purpose of determining if participation in the COVID-19 rapid testing program is required.

Individuals who declare they are fully vaccinated are required to provide proof of vaccination; those who do not declare they are fully vaccinated are required to provide proof of testing.

The overall purpose of the program is to maintain the health and safety of UBC students, faculty and staff.

Systems

The process for identifying those requiring rapid testing (initially declarations), scheduling rapid tests, and collecting associated test results will be managed using a cloud solution operated by Thrive Health.
Thrive Health, founded in 2016, is a company that has developed healthcare solutions within Canada. They developed the BC COVID-19 Support App for the BC Government and Ministry of Health, and they have developed an app to support Canadian universities that have introduced or are in the process of introducing mandatory COVID-19 rapid antigen screening programs.

Rapid Screening Clinics

A dedicated COVID Rapid Screening (aka Rapid Test) clinic has been set-up on each of the UBC Vancouver and Okanagan campuses to support this project. Participants who must provide proof of testing can use the Thrive application to schedule appointments for testing at their respective clinics.

RISK CLASSIFICATION

The inherent privacy risk classification level of this PIA submission is **4 – High**.
The residual risk classification level at closure of each phase or iteration is as follows:

Version	Inherent Risk	Risk Level	Remarks & Observations
1.0	4 – High	1 - Low	Declaration of vaccination status
2.0	4 – High	3 - Medium	▪ Ability for participants to upload evidence of vaccination ▪ Ability to book appointments at testing clinic ▪ Reports and extracts to support new functionality ▪ Broadcast e-mails to students and employees ▪ Recording of rapid test results ▪ Reporting of positive tests to health authorities

1.3 Scope of PIA

This PIA considers all collection, use and disclosure of information associated with the vaccination declaration, collection of evidence of vaccination and test results (when required). The PIA considers all data flows associated with personal health information collected/used as part of the program.

This PIA will be delivered in versions, aligned with the program delivery phases.

- The first version considered the platform supporting the process (Thrive Health), and a declaration of vaccination status.
- The current version addresses initial uploading of one's proof of vaccination, scheduling a rapid testing appointment, administrative reporting requirements, and e-mail communications

In preparing this PIA, we considered and, where appropriate, applied the principles set out in the **Joint Statement by Federal, Provincial and Territorial Privacy Commissioners on Privacy and COVID-19 Vaccine Passports** (https://www.oipc.bc.ca/media/17359/2021-05-19-fpt-joint-statement-vaccine-passports.pdf).

1.4 Related PIAs

An expedited privacy review was conducted in Spring 2021 on the Thrive Health application in relation to a UBC research project.

1.5 Elements of Information or Data

UBC will handle the following types of personal information for program participants:

- UBC Identity Data,
- Vaccination Declarations,
- Location Data,
- Vaccination Evidence,
- Rapid Test Data

The below data definitions describe the attributes collected for each type of personal information listed above:

UBC Identity Data

- First Name
- Last Name
- Preferred name
- Email Address
    - For students this will be either
        - UBC assigned @student.ubc.ca e-mail address, or
        - their preferred personal e-mail address provided by the student to SIS
    - For employees this will be either
        - UBC assigned e-mail address if available, or
        - Personal e-mail address provided by the employee to HR
- Student Number
- Employee Number
- UBC Affiliation – one or more of
    - Student
    - Faculty
    - Staff

    - Alumni
    - Member
    - Affiliate – theological college students
    - Employee – Contractors, Guests, Contingent Workers, Paymaster Workers
- Student housing indicators
    - Resides in student housing
    - Resides in single occupancy unit
- Varsity athlete indicator
- Allowed to book appointment indicator
- SP-PUID identifier

Vaccination Declarations
Participants' declarations of vaccination status (fully vaccinated, partially vaccinated, unvaccinated, prefer not to say).

Location Data
Data collected about participants' location (campus, another UBC facility, whether or not returning to campus).

Vaccination Evidence
Participants who have attested they are fully vaccinated will be required to upload an image or file in .PDF, .JPG, or .PNG format evidencing they are fully vaccinated.

- If eligible, they must provide their BC Vaccination Card
- If not currently eligible for BC Vaccination Card, they must provide other official documentation that shows full name, name of vaccine(s), date(s) administered. If vaccinated outside of Canada, proof of vaccination which was required in order to enter Canada.

Rapid Test Data
- Rapid Screening clinic appointment scheduling information, including date, time and location of scheduled appointments of individual participant, and status of scheduled appointment (booked, fulfilled, no show, etc.) of individual participant
- Results of rapid tests administered to the individual participant

Note: Additional information and consents are collected on-**site in accordance with BC Public Health and PHSA clinic operations requirements and standards. In the event of a positive test, additional information about the participant will be collected and shared with the local Health Authority.**

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

The Thrive Health application stores data on Amazon Web Services servers located in Canada. In addition, it may store personal information of users outside of Canada as follows:

- If consented by the user, Thrive Heath will send messages to the user for marketing purposes. These messages will use a US-based mail server.
- The application features authentication services, Auth0 and Gmail, which store data outside Canada. UBC is not using these services as part of this implementation.
- Technical support requests are routed to support staff located in the United States. This could result in storage of support emails and addresses outside Canada.
- Email notification instructing users to access the Thrive Application utilize a service provider that processes or stored information outside Canada.

Any sharing of personal information outside Canada that might occur would be authorized under section 33.1(1)(b) and section 33.1(1)(p) of FIPPA.

The following table outlines UBC's analysis of all information Thrive Health has stated in its Privacy Policy to be shared with third party services.

PROVIDER	DATA THAT IS SHARED	USAGE / PURPOSE	UBC ANALYSIS
AMAZON WEB SERVICES (CANADA)	▪ Not applicable	Thrive Health uses **AMAZON WEB SERVICES** (AWS) located in Canada to provide infrastructure services to host their software platform. Thrive Health's business agreement with AWS prevents Amazon from accessing your data that is stored on the Thrive platform. In addition, Thrive Health encrypts your data using encryption keys held by them.	Not applicable.
AMPLITUDE (USA)	▪ IP address ▪ Randomly generated identifier(s) ▪ User event data	**AMPLITUDE** is a solution that consumes the product usage metrics collected using SEGMENT *(see below)* and allows Thrive Health's product team to analyze those metrics to generate insights and reports. The data that is shared is considered metadata.	Please refer to the assessment notes for SEGMENT below.
AUTH0 (USA)	▪ E-mail address ▪ Password hash	**AUTH0** provides user account management and authentication system. If you have created a Thrive Health account your email address and a cryptographic hash of your password are stored in AUTH0. None of your health information is shared with AUTH0 If you use your UBC CWL to log-in to Thrive Health, no UBC information is shared. The UBC CWL log-in process uses Thrive-specific identifiers which not identify you.	Not applicable. UBC does not use AUTH0 for the CWL login process.
GOOGLE ANALYTICS (USA)	▪ IP address (masked) ▪ User event data	**GOOGLE ANALYTICS** provides application usage metrics similar to AMPLITUDE. IP addresses collected by GOOGLE ANALYTICS are automatically masked to preserve anonymity. This data is considered metadata.	Application usage metrics that are not identifiable do not constitute personal information.
MAILCHIMP (USA)	▪ E-mail address	Thrive Health's marketing team uses **MAILCHIMP** to manage email campaigns. If you have opted-in to receiving occasional product updates from Thrive Health, they will use MAILCHIMP to send you email.	Participants consent to this disclosure if and when they opt-in to receive marketing and product updates.
SEGMENT (USA)	▪ IP address ▪ Randomly generated identifier(s) ▪ User event data	**SEGMENT** is a service that allows us to collect application usage metrics in a standardized way. These usage metrics allow us to better understand how our products are being used and improve our platform. The randomly generated identifier(s) are used to uniquely identify your user event data. These identifiers cannot be used to identify you, or tie this user event data back to your personal identity.	This information is metadata and not personal information.
SENDGRID (USA)	▪ E-mail address	**SENDGRID** is a transactional email service that Thrive Health uses to send email notifications and alerts to you from their core platform.	This feature is not used in the current phase of the project.
ZENDESK (USA)	▪ E-mail address ▪ Technical support request	**ZENDESK** is used to manage customer support requests from Thrive Health users	Although email addresses of students can contain personal information, most UBC students have consented to disclosure of their UBC email. Further, users have also consented to this disclosure as part of the Thrive Health Privacy Notice.

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 Common or Integrated Program or Activity

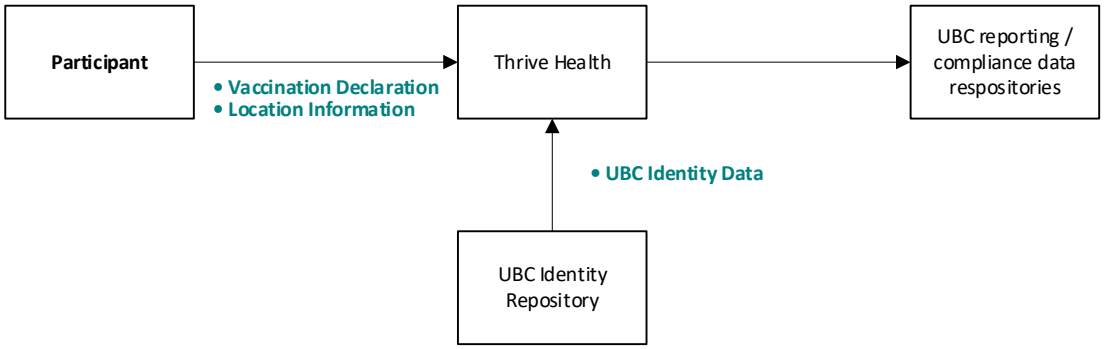
In FIPPA, "common or integrated program or activity" is strictly defined; where one exists, it must comply with requirements under the Act for common or integrated programs and activities.

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

Authentication/Account Creation & Declaration Data Flow



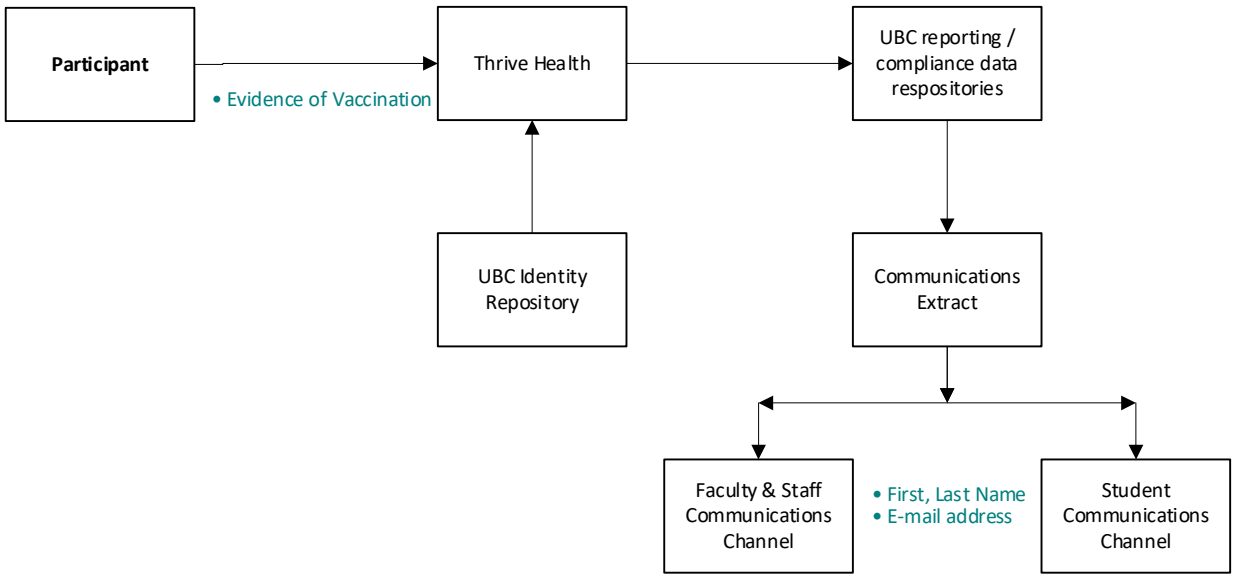
- Authority to collect from participants is section 26(c) of FIPPA
- Authority to disclose to Thrive Health is section 33.1(1)(e.1) of FIPPA

Reporting/Compliance Data Flow

Reports are currently limited to those required by the UBC IT implementation team to support roll-out of each phase of the initiative. Aggregated reports are provided to assist in reporting / compliance planning. Detailed compliance reports are planned for later phases of the program.

All internal disclosures, which are for the purposes of technical support, communications, troubleshooting and statistical purposes, adhere to the need-to-know principle.

Vaccination Evidence Data Flow



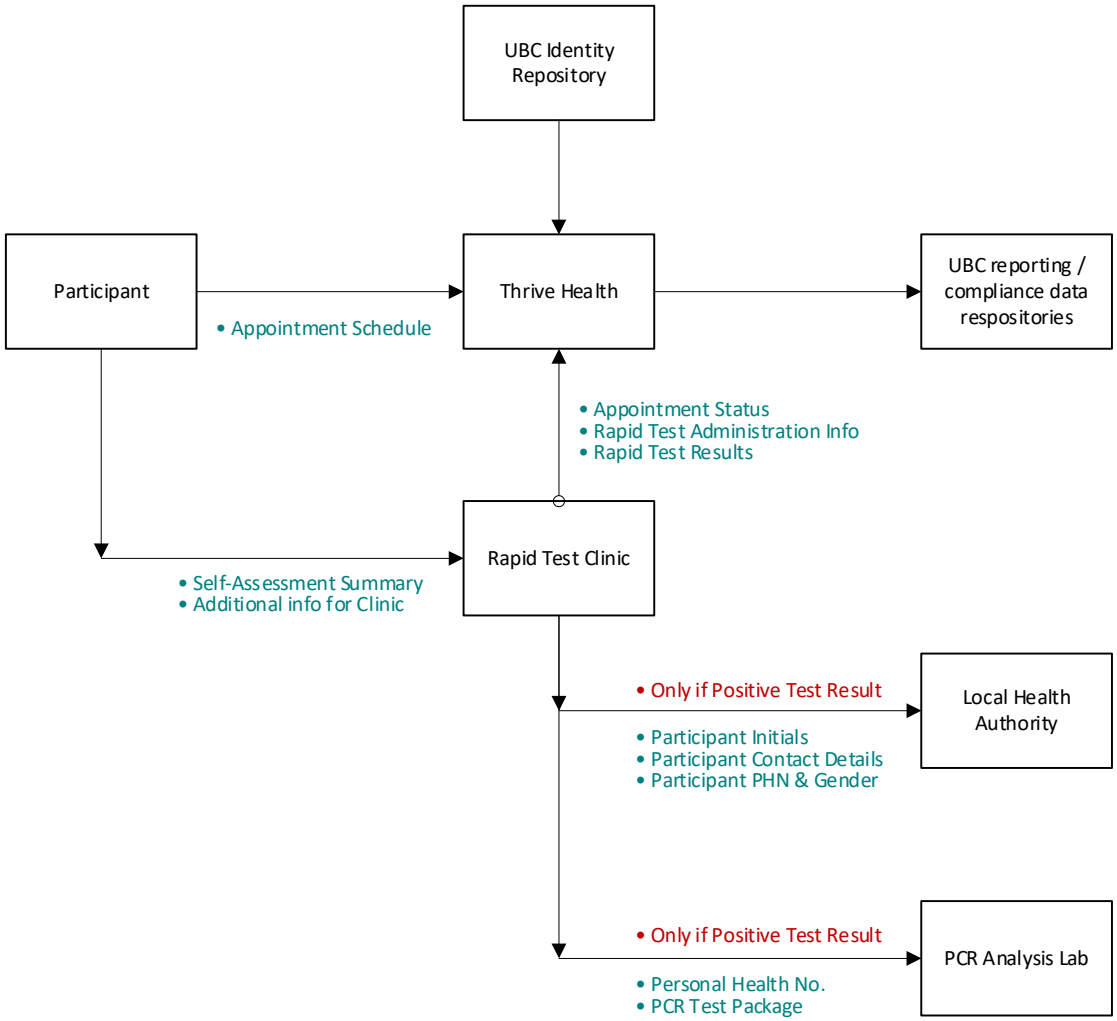
UBC collects and retains evidence of vaccination for the purpose of this initiative under the authority of section 26(c) of FIPPA.

We have reviewed the relevant legislation and Public Health Orders and have concluded that there are no legislative or regulatory restrictions on the collection of proof of vaccination, including the BC Vaccine Card, for the purposes of UBC's initiative.

We have noted that there are two Public Health Orders that prohibit the retention of proof of vaccination in specified circumstances: The Order on Food and Liquor Serving Premises (https://www2.gov.bc.ca/assets/gov/health/about-bc-s-health-care-system/office-of-the-provincial-health-officer/covid-19/covid-19-pho-order-nightclubs-food-drink.pdf) prohibits operators of such premises from retaining proof of vaccination and the Order on Gatherings and Events (https://www2.gov.bc.ca/assets/gov/health/about-bc-s-health-care-system/office-of-the-provincial-health-officer/covid-19/covid-19-pho-order-gatherings-events.pdf) contains an identical prohibition that applies to organizers of certain gatherings and events. However, neither of these Orders applies to UBC's proof of vaccination initiative. We understand that UBC has notified the provincial health authorities that it will be collecting and temporarily storing proof of vaccination in the course of this initiative and that the preferred form of proof will be the BC Vaccine Card.

UBC considered the option of manually checking each proof of vaccination without collecting an image, but rejected this option for two reasons. First, manually checking 80,000 or more vaccination cards would raise significant cost and logistical challenges. Second, a large number of managers and staff across the organization would have to be assigned to collect this information, which would be unacceptably privacy-invasive. We agree that the collection of images of vaccination cards and the review of these images by a small project team is a more privacy-sensitive approach, provided that the images are stored securely and destroyed reasonably quickly after the verification process.

Rapid Test Data Flow



UBC collects personal information from each individual who attends the Rapid Screening clinic under the authority of section 26(c) of FIPPA.

In the event of a positive test result, UBC discloses the personal information of the specific individual to the Provincial Health Services Authority (PHSA) and the relevant local health authority (Vancouver Coastal Health Authority or Interior Health Authority). UBC discloses this information under the authority of section 33.1(1)(c) of FIPPA.

2.2 Risk Mitigation Table

The following table outlines risk identified in relation to the project and recommended response plan.

Risk	Ref#	Inherent Likelihood	Inherent Impact	Response	Residual Risk
Over collection of personal information Personal information is collected without legal authority	RK0020872	4 – High	4 - Major	Mitigate	3 – Medium
	Mitigation Plan: Under section 26(c) of FIPPA, personal information may be collected if it "relates directly to and is necessary for a program or activity of the public body". In this case, information is being collected for the purposes of health and safety programs of the University. UBC has traditionally taken a conservative approach to health and safety, and this approach is reflected in relatively rigorous standards that it applies in its health and safety programs. We are informed that the personal information being collected in this case relates directly to and is necessary for ensuring that UBC complies with these rigorous standards. In our opinion, the program collects the minimum amount of information necessary to accomplish these purposes. As such, the collection is authorized under section 26(c) of FIPPA.				
Personal information stored / accessible outside of Canada Data handled by the program (specifically Thrive, subservice providers and integrations) could result in disclosure or storage outside Canada.	RK0020869	4 – High	4 - Major	Mitigate	2 – Low
	Mitigation Plan: Although the designed UBC use of Thrive Health in the first phase should not result in storage of personal information outside Canada, there are circumstances in which this may occur. See section 1.6 for current mitigations and analysis. Any sharing of personal information outside Canada that might occur would be authorized under section 33.1(1)(b) and (p) of FIPPA.				
Retaining personal information longer than necessary Retention practices for personal information have not yet been developed, resulting in possible retention of personal information longer than necessary.	RK0020871	4 – High	3 – Significant	Mitigate	3 – Medium
	Mitigation Plan: The program team must establish and implement retention and disposal processes / practices for personal information stored in Thrive and paper repositories, considering: ▪ The requirement under section 31 of FIPPA to retain personal information used to make a decision for at least a year, ▪ The principle that personal information should not be retained longer than reasonably required to accomplish the purpose. .				
Weaknesses within information security controls Systems and configurations associated with program delivery have control weaknesses that could result in an information security breach.	RK0020875	4 – High	3 - Significant	Mitigate	2 – Low
	Mitigation Plan: Thrive Health has provided evidence that has established to our satisfaction that reasonable security measures are in place for in-scope services. In addition, UBC's storage and access procedures are satisfactory. The following information security controls should be considered/reviewed to further ensure security for the program: • Administration login portals should have access restricted to white-listed IP ranges. • Permissions for locations used for storage of reporting/ compliance data repositories should be limited to those who need to know. • All access requests to personal information (within Thrive and UBC reporting / compliance data repositories) must be authorized by a process approved by the steering committee. • Transmission of compliance reports must use secure methods. • Email notifications in subsequent phases should avoid use of direct HTML links, and should direct users to navigate to the UBC landing page. • Content of e-mail notifications / reminders and existence of such e-mails should be limited to only those with need-to-know, in particular within the SIS environment. • Physical security control over paper records are required.				
Use of personal information	RK0020874	4 – High	3 – Significant	Mitigate	2 – Low

Risk	Ref#	Inherent Likelihood	Inherent Impact	Response	Residual Risk
for an alternate purpose Personal information may be used for a purpose beyond that for which it was originally collected.	**Mitigation Plan:** UBC has collected information for the specific purpose of determining whether participants are required to participate in the COVID-19 rapid testing program and investigation or disciplinary purposes where necessary. No additional use should take place without additional Privacy Impact Assessment. According to Thrive Health's Privacy Notice it only uses personal information collected for purposes connected with the above purposes. It should also be noted that Thrive Health uses de-identified data (which is not personal information) for other purposes, such as for statistical analysis and to improve its services.				

2.3 Collection Notice

The following notice is provided to participants in this program:

> The personal information you provide in this self-declaration is being collected under the authority of section 26(c) of BC's Freedom of Information and Protection of Privacy Act (FIPPA). This information will be used for the purpose of determining whether you are required to participate in the COVID-19 rapid testing program and may also be used for investigation or disciplinary purposes related to this program. De-identified aggregated information will also be used to track the overall vaccination status of the UBC community.
>
> Staff and faculty questions about the collection and use of this information may be directed to hr.info@ubc.ca; and student questions about the collection of this information may be directed to:
>
> - UBC Vancouver Campus Students: vicepresident.students@ubc.ca
> - UBC Okanagan Campus Students: avps.ok@ubc.ca

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

See section 1.6 above. UBC obtained consent is not required.

2.5 Consent Withheld Procedure

Not applicable. UBC obtained consent is not required.

PART 3: SECURITY OF PERSONAL INFORMATION

3.1 Physical Security Measures

Thrive Health relies on the services provided by AWS Canada for physical protection of its infrastructure. In our opinion, AWS meets or exceeds UBC's physical security requirements in UBC Policy SC14 (Information Systems Policy) and Information Security Standard M9 - Physical Security of UBC Datacenters. Therefore, the physical security measures comply with section 30 of FIPPA.

Mitigations in relation to physical security over paper records are specified in the Risk Mitigation Table.

3.2 Technical Security Measures

UBC Policy SC14 and UBC Information Security Standards are met or exceeded by the policies and practices documented by Thrive Health. This has been evidenced through analysis of Thrive Health's SOC 2 type I, and Thrive Health's provision of a Higher Education Community Vendor Assessment Toolkit.

While current measures are sufficient to comply with section 30 of FIPPA, specific additional measures are recommended within the risk table of this report to further secure personal information handled through the project.

3.3 Security Policies, Procedures, and Standards

UBC Policy SC14 and UBC Information Security Standards, as well as the applicable Thrive Health procedural documents, comply with section 30 of FIPPA.

Thrive Health is ISO/IEC 27001 certified.

3.4 Tracking Access / Access Controls

UBC has implemented a highly centralized process for managing the program. Very limited central (HR/Student Support and Safety & Risk Services) administrators control the application and have access to data. All access requests will be reviewed to ensure only minimal necessary access will be granted. This also includes access to data extracts and reports.

Access and changes to the contents of records, and changes to access authorities are logged.

Thrive Health Technical Support
Thrive Health technical support has direct access to all data within the application on an as-needed and need-to-know basis, for the purposes of technical support and troubleshooting. Such accesses are aligned with provisions within FIPPA.

UBC Project Manager and Administrators
The UBC project manager has access to specific data, as appropriate, via extract reports provided by the UBC IT implementation team, for the purposes of managing the project, validating delivery of functionality, and managing issues.

Project administrators have access to specific reports, as approved by the Steering Committee and provided via the Project Manager, for the purposes of administering delivery of the project, providing communications to participants, etc.

UBC IT Implementation Team
The UBC IT implementation team has access to specific data via extract files as required for the implementation process, verification of functionality and processes, development of UBC reports for the project manager and administration.

Access Roles Within Thrive Health Application
Specific individuals responsible for the overall management and administration of the COVID Testing & Proof of Vaccination project are assigned Organization Administrator or Set-Up Administrator access roles within the Thrive Health application per their duties and responsibilities. These roles have access to personal information of participants as indicated in the table below.

Rapid Screening clinic managers and staff are assigned Organization Coordinator, Rapid Screening Coordinator, or Vaccination Coordinator access roles within the Thrive Health application per their assigned duties and responsibilities within the clinic. These roles each have access to the personal information of participants as indicated in the following table.

UBC Access Roles Within Thrive Health Application	View administrators	Add & edit administrators	View & export reports	View individuals	Add & edit individuals (manually)	Add & edit individuals (bulk)	Edit system configuration settings	Create & edit locations	Create & edit schedules	Create & edit registration codes	Create & edit groups	View self-assessment, test results	Add test results	View appointments	Add, edit & check-in appointments	View vaccination form & status
Organization Administrator	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	
Set-Up Administrator	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓					
Organization Coordinator				✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	
Rapid Screening Coordinator				✓	✓								✓	✓	✓	
Vaccination Coordinator				✓												✓

Access for Compliance or Disciplinary Matters

In the event of a compliance or disciplinary matter, the personal information about a given participant may need to be shared within UBC on a strictly need-to-know basis.

PART 4: ACCURACY, CORRECTION, AND RETENTION

4.1 Updating and Correcting Personal Information

Not applicable.

4.2 Decisions That Directly Affect an Individual

Responses provided by the individual and recorded in the Thrive Health application will be used to make decisions which directly affect the individual. This is outlined in the privacy notification and instructions which are provided to individuals both on the landing page and at the points of submission of test results and declaration.

4.3 Records Retention and Disposal

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

Information provided by individuals, such as test results or vaccination declarations may be used for decisions which directly affects an individual and must therefore be retained for at least one year as per FIPPA

Mitigations in relation to retention risk are specified in the Risk Mitigation Table.

PART 5: FURTHER INFORMATION

5.1 Systematic Disclosures of Personal Information

This program does not involve the systematic disclosure of personal information.

Personal information of a given participant is disclosed to PHSA, the respective local Health Authority, and the PCR testing lab only in the event of a positive COVID antigen test result.

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

The current phase of the program delivery is subject to BC and Canada Public Health legislation in regards to reporting and disclosure of information related to infectious diseases.

The initiative is also subject to BC Public Health Orders related to collection, recording, and disclosure of personal information and personal health information in relation to the COVID-19 pandemic.

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. Materials reviewed related to Thrive Health included:

- privacy and security policies, statements, and documents publicly available from Thrive Health
- privacy and security documentation provided by Thrive Health under license or Non-Disclosure Agreement
- security assessment reports provided by 3rd parties under license or Non-Disclosure Agreement
- assessments shared from other Thrive Health clients under Confidentiality and/or Non-Disclosure Agreements

The following specific documents have been relied upon as part of this PIA:

Information Reviewed	Date Received
Thrive Health HECVAT (Full Responses)	2021-09-01
Thrive Health 2020 SOC 2 Type i	2021-08-31
Thrive Health Workplace - Rapid Screening & Vaccine Status Reporting	2021-08-30
Thrive Health – Terms of Use	2021-09-03
Thrive Health - Privacy	2021-09-03
Thrive Health - Privacy Notice	2021-09-03
Contract Amendment – Appendix D – Vaccine Status Registry	2021-09-05
BitSight Report – Thrive Health	2021-09-01
Joint Statement by Federal, Provincial and Territorial Privacy Commissioners on Privacy and COVID-19 Vaccine Passports	2021-08-31

6.2 Analysis and Findings

The information provided for the review has established that Thrive Heath can be used in the manner proposed within this PIA in compliance with FIPPA and UBC's Information Security Standards.

The following are the key factors in that determination:

- Personal information is collected with proper authority;
- Any sharing of personal information outside Canada that might occur would be authorized under section 33.1(1)(b) and (p) of FIPPA;
- Personal information is not disclosed to third parties;
- Personal information is kept secure during transmission and at rest;
- Access to personal information is limited and requires use of a valid login credentials with appropriate access authorities.

6.3 Conditions of Approval

Condition #1

The program team must establish and implement retention and disposal processes / practices for personal information stored in Thrive and paper repositories, considering:

- The requirement under section 31 of FIPPA to retain personal information used to make a decision for at least a year.
- The principle that personal information should not be retained longer than reasonably required to accomplish the purpose.

Condition #2

The following information security controls should be considered/reviewed to further ensure security for the program:

- Administration login portals should have access restricted to white-listed IP ranges.
- Permissions for locations used for storage of reporting/ compliance data repositories should be limited to those who need to know.
- All access requests to personal information (within Thrive and UBC reporting/ compliance data repositories) must be authorized by a process approved by the steering committee.
- Transmission of compliance reports must use secure methods.
- Email notifications in subsequent phases should avoid use of direct html links, and should direct users to navigate to the UBC landing page.
- Content of e-mail notifications / reminders and existence of such e-mails should be limited to only those with need-to-know, in particular within the SIS environment
- Physical security control over paper records is required.

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 personal information collection or use will require a new PIA.

Acceptance of Assessment

This refers to the Owner's acceptance of the assessment as presented at each major iteration of this report as the Initiative and PIA progress. The major iterations are outlined in the *PREFACE* section, which appears at the beginning of this document.

Version	Accepted On	Assessment Accepted By	Title / Position
1.0	2021-09-13	Rae Ann Aldridge	Executive Director, Safety & Risk Services
2.0	2021-10-08	Rae Ann Aldridge	Executive Director, Safety & Risk Services

Report Distribution

This refers to distribution of the report for review and/or acceptance of the assessment. The report may have also been distributed to a broader audience for the purposes of information only; however, that audience is not necessarily recorded here.

Distributed to	Name	Title / Position
Business Owner	Aldridge, Rae Ann	Executive Director, Safety & Risk Services
Project Manager	Questa, Jamiann	Director, SRS Environmental Protection
PIA Requestor	Lonsdale-Eccles, Michael	Director, SRS PrISM
Legal Counsel	Hancock, Paul	Legal Counsel, Information and Privacy
SRS PrISM Risk Advisor	Tremonti, Robert	Lead Advisor, Privacy and Information Security Risk