UVic COVID-19 Rapid Testing Program Privacy Impact Assessment

Author and Contact Information	David To, Privacy and Access to Information Officer, privacyinfo@uvic.ca
Reviewed By	Bradley Weldon, Chief Privacy Officer, privacyinfo@uvic.ca
Review Date	September 23, 2021

Purpose:

The purpose of the Privacy Impact Assessment (PIA) is to assess risks associated with how a project plans to handle personal information. The purpose of the PIA is to ensure the project approach will be compliant with the policy and legislative requirements, and that any risks to privacy are mitigated, or, if they cannot be completely mitigated, understood and accepted by the appropriate Administrative Authority as defined in section 2.00 of Policy IM7800:

> *Administrative Authority means individuals with administrative responsibility for units (e.g., Vice-Presidents, Chief Information Officer, Executive Directors, Deans, Chairs, Directors and other unit heads) and individuals with functional stewardship of university Information Resources.*

Roles:

The role of University Systems is to complete this document and provide guidance regarding security policy compliance and risks to the Administrative Authority.

The role of the Privacy Office is to review this document and provide guidance regarding privacy policy, legislative compliance and risks to the Administrative Authority.

The Administrative Authority is accountable for ensuring the Information Resource being implemented or changed, as a result of this project, is compliant with privacy and security policies and legislation and accepting risks associated with non-compliance on behalf of the institution.

1.0 Privacy Context

1.1 Description

Effective September 10, 2021, the University of Victoria will be implementing a COVID-19 Rapid Testing Program. This will be handled through Thrive, an application that will collect student and employee name, e-mail, and V-number from UVic's single-sign-on service (SSO) and will ask individuals to declare their COVID vaccination status. Individuals who are vaccinated are exempt from the testing protocol. Should the individual attest that they have not received both COVID-19 vaccinations (or prefer not to say), then they will be prompted to make an appointment at a rapid testing site on campus to determine if they have COVID-19 prior to attending any activities on campus.
As an update to the system, when a student declares that they are either fully vaccinated or partially vaccinated they will be asked to submit photo proof of their status. These will be randomly audited at regular intervals to verify authenticity but an audit team consisting of three (3) individuals.

1.2 Privacy Issues Related to this Project

Students and staff will be required to provide the University with their contact information and vaccination status. The privacy issues related to this are:

- **Storage and access of personal information inside and outside of Canada;**
- **Collection and security of personal health information;**
- **Contacting individuals that need to make appointments for testing; and**
- **Tracking attendance at testing appointments.**

1.3 Privacy Impact Assessment Scope

The scope of this PIA will cover:

Project Scope	Privacy-Related Activities and Processes
The collection of vaccination status of students and employees	• Individuals will log into the Thrive app via SSO and enter their vaccination status. This can be one of four options: vaccinated, partially vaccinated, not vaccinated or 'prefer not to say'. • If status is 'vaccinated' then no further collection is required. Otherwise, individuals will be required book appointments to submit to a COVID-19 test on a weekly basis.
The declaration that a student or employee agrees to comply with mask policies while on campus	• Individuals must declare that they have read and agreed to adhere to the mask policy while on campus. Collection of this information will be done by having the individual check a box saying that they agree to the declaration.
Random vaccination audits conducted by the audit team to confirm vaccination status of Thrive Users	• Individuals who are either partially vaccinated or fully vaccinated will be asked to provide proof of vaccination to the Thrive App. These will be randomly audited at regular intervals by the audit team.

1.4 Related Privacy Impact Assessments

None

1.5 Elements of Information or Data

Data	Description	Usage
Name	First and last name	
Phone number	Users will be asked to input a phone number	The last 4 digits will be used to verify the identity of the user.
V number	Employee/student unique identification number	Number will be used to create a unique record for the individual.
Vaccination Status Attestation	Whether or not individual is vaccinated	Users will be asked if they are fully vaccinated, partially vaccinated, or not vaccinated at all. If fully vaccinated, then they will be exempt from the Rapid Testing appointment.
Appointments for Testing	Rapid Testing clinic appointment	Individuals will make appointments on Thrive at the UVic testing clinic. Fully vaccinated individuals are exempt from this process.
Mask Policy Attestation	A checkbox to confirm that an individual has read and agrees to abide by mask policies while on campus	To acknowledge that the individual is aware of the mask policies while on campus.

2.0 Protection of Personal Information

2.1 Storage or Access outside of Canada

Vaccination status and testing appointment information are stored inside Canada.

Thrive uses Auth0 to provide SSO functionality. Auth0 stores username, Netlink ID, V-number, email and affiliation with UVic (e.g., faculty/staff/student) on its secure servers, outside of Canada. For UVic employees, this information is considered contact information as defined by Schedule 1 of FIPPA and is therefore not personal information. The storage of this student personal information outside of Canada is authorised by Ministerial Orders No. M431 of the Minister of Citizens' Services.

Thrive uses SendGrid to provide email functionality. These emails confirm rapid testing appointments. This is information disclosed outside of Canada to SendGrid for the purpose of processing, as authorised by s33.1(p.1) of FIPPA.

2.2 Personal Information Flow Diagram and/or Personal Information Flow Table

Personal Information Flow Table			
	Description/Purpose	**Type**	**FIPPA Authority**
1.	*User logs into THRIVE for the first time using SSO. UVic discloses username, Netlink ID, V-number, email and affiliation of individual with UVic to Thrive.* *Contact information is collected.*	*Disclosure* *Collection*	*33.2(c)* *33.1(1)(c)* *26(c)*
2.	*User reads Mask Policy and checks a box to confirm.*	*Collection*	*26(c)*
3.	*User is asked to declare their vaccination status: fully vaccinated, partially vaccinated, not vaccinated, or prefer*	*Collection* *Disclosure*	*26(a),(c),(e)* *33.2(c)*

	not to say. If vaccinated or partially vaccinated, they will be asked to provide proof through the app.		*33.1(1)(c)*
4.	*Users will use THRIVE to book appointments for COVID-19 testing. They will receive a QR code that they will be able to use at their appointment to confirm their arrival.* *If the individual is fully vaccinated, then they are exempt from this and all subsequent steps.*	*Collection*	*26(a),(c),(e)*
5.	*Rapid Testing Coordinators and nurses will scan a user's QR code or ask for more information to verify the identity of individuals and confirm that they have arrived for their appointment*	*Use*	*32(a)*
6.	*If an individual has missed their appointment, then they may be contacted to remind them that it is mandatory to submit to a COVID-19 rapid test.*	*Use*	*32(a)*
7.	*A random audit will be conducted by the audit team to verify proof of vaccination of individuals.*	*Use*	*32(a)*

Collection Notice

When an individual accesses the Thrive App, they are provided the following collection notice before they can input their information:

The personal information that you provide is being collected by Thrive Health Inc. on behalf of the University of Victoria under the authority of the *University Act* and section 26 (a), (c), and (e) of the *Freedom of Information and Protection of Privacy Act*. Your personal information will be used to manage the health and safety of individuals attending activities on campus during the COVID-19 pandemic. This includes determining whether you are required to participate in the COVID-19 rapid testing program and for investigation or disciplinary purposes, including the determination of interim measures, related to this program. De-identified aggregated information will also be used to track the vaccination status of the UVic community. If you have any questions about the collection and use of your personal information, please contact the Chief Privacy Officer at privacyinfo@uvic.ca.

2.3 Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Unauthorized access to individuals' personal information.	Access to this information is restricted to four admin level staff only, with fine-grained, role-based access within admins. Audit logs record all access to personal information.	Low	Medium
2.	Thrive may be subject to cyber-attack and privacy breach.	Thrive has ISO27001, ISO27017, ISO27018 information security controls in place, and is required to maintain those certifications for the duration of the program.	Low	Medium

		Thrive is required to report to UVic any actual or suspected breach of personal information and cooperate with UVic to investigate and mitigate such a breach.		

3.0 Security of Personal Information

3.1 Please describe the physical security measures related to the initiative (if applicable).

THRIVE has security policies and standards in place which are reviewed, updated as required, approved by senior management and communicated to relevant stakeholders annually.

Further information can be found in Appendix A (attached)

3.2 Please describe the technical security measures related to the initiative (if applicable).

THRIVE has the ISO27001, ISO27017, and ISO27018 information security certifications.

Further information can be found in Appendix A (attached).

3.3 Does your department rely on security policies other than the Information Security Policy?

THRIVE is required by contract, to implement the Information Security and Security Incident Notification policies found in Appendix A (attached).

3.4 Please describe any access control and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

UVic has implemented strict role-based access:

- Four Organization Administrators with access to users name, vaccination status, V-number, and Rapid Testing appointment attendance; and
- Four Rapid Testing Coordinators with access to users name and appointment attendance.
- Three Auditors with access to vaccination status and users name

Access to each record is logged to ensure only those records are accessed which are necessary for the performance of the duties of the administrator or coordinator.

3.5 Please describe how you track who has access to the personal information.

All actions performed in the Thrive App will have audit logs. This includes records that admin level staff may view.

4.0 Accuracy/Correction/Retention of Personal Information

4.1 How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the university notify them of the update, correction or annotation?

Individuals may update or correct their vaccination status via Thrive App. Since users will be signing on using their UVic SSO credentials, should they wish to update their personal contact information, they can contact UVic Systems HelpDesk for assistance.

At the end of UVIC's contract with THRIVE, all user personal information will be deleted from THRIVE's servers.

4.2 Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

Individuals who are not fully vaccinated or prefer to not declare their vaccination status must be tested weekly for COVID-19 at the UVic Rapid Testing Clinic.

4.3 If you answered "yes" to question 4.2, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

Users self-declare their vaccination status and can update their status as needed.

4.4 If you answered "yes" to question 4.2, do you have an approved records retention and disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

A review in relation to the UVic Directory of Records is in progress. Personal information used to make a decision that directly affects an individual will not be deleted prior to the completion of that review.

5.0 Further Information

5.1 Does this initiative involve systematic disclosures of personal information? If yes, please explain.

No.

5.2 Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

UVic will use information about vaccination status for aggregate statistical reporting and planning of vaccination and Rapid Testing Clinics.

5.3 Will a personal information bank (PIB) result from this initiative?

Yes.

Appendix A: Security Requirements

1. Introduction

a) This Appendix C describes the security requirements to which the Software and the Services provided under this Agreement will at all times strictly comply.

b) Unless otherwise expressly provided hereunder, all Section references in this Schedule are references to Section numbers of this Schedule and not to Sections of other parts of this Agreement.

2. Definitions

a) In this Appendix C, the following capitalized terms and expressions have the following meanings:

"Cloud Services" means the cloud services used by THRIVE Health in support of, and to operate, the Software;

"Organization Systems" means the Organization computer systems and network; and

"Security Incident" means any loss of, unauthorized access to, unauthorized use, unauthorized disclosure or inability to account for Personal Information including when resulting from a breach of THRIVE Health's or its suppliers' security safeguards or from a failure to establish those safeguards.

b) Capitalized terms and expressions not otherwise defined in this Appendix C have the terms that are ascribed to them in the main body of the Agreement or, in the absence of definition within the main body of the Agreement, such capitalized terms and expressions will have the generally accepted industry or technical meaning given to them.

3. Organizational Security

3.1. Security Program Management

a) THRIVE Health has in place security policies and standards which are reviewed, updated as required, approved by senior management and communicated to its relevant internal stakeholders at least annually.

b) THRIVE Health shall maintain a formalized security risk management framework including documented processes for assessing internal and external risks (including third parties and supply chain) and determination of risk treatment;

c) THRIVE Health shall ensure that the Cloud Service and Infrastructure used to manage the Cloud Service and Infrastructure and all data centers used in providing the Cloud Service and Infrastructure (including for management, back-up or disasterrecovery purposes) are compliant with one of the following international established cloud security frameworks: ISO 27017, NIST 800-53, CSA Cloud Controls Matrix (CCM);

d) THRIVE Health shall provide third party attestation of their security controls (e.g. ISO / SOC Compliance Report) to the University of Victoria annually for the duration of the service agreement.

3.2. Employment Screening

a) THRIVE Health shall ensure all employees, contractors, and third parties granted access to its own physical locations, systems and data are subject to background checks as permitted by local laws, regulations and contractual constraints, and will be subject to non-disclosure or confidentiality agreements as a condition of employment.

3.3. Security Training and Awareness

a) THRIVE Health has in place and will maintain a formal security awareness program for all employees, contractors and appropriate third parties which includes at minimum (i) cloud related access and data management issues; (ii) addresses the responsibilities of employees with regard to security and data integrity; and (iii) ensures awareness

of responsibilities including maintaining compliance with internal policies and standards, applicable legal requirements, and maintaining a safe and secure physical environment.

4. Access and Systems

4.1. Access

a) THRIVE Health has in place industry best practices with respect to strategies and standards to appropriately secure, and restrict physical and logical access (as applicable) to equipment, software, networks, and Information utilized in connection with the provision of the Software through the application infrastructure.

b) The Parties acknowledge and agree that THRIVE Health uses the hosting services of third party cloud services providers THRIVE Health shall ensure that adequate contractual provisions are in place with such services providers, in accordance with Section 4.1 (a) hereto.

4.2. Change in Location

While under THRIVE Health's control and responsibility, the Information shall at all times remain in the Territory. THRIVE Health will not transfer any of its operations relating to access to, storage, hosting, handling or use of the Information in the provision of the Software to any other location without the prior written notification of the Organization.

5. Organization System and Information

5.1. Access Control

a) THRIVE Health will:

i) only provision access to the Organization Information to individuals who have a legitimate need and only after formally authorized by a designated approver as defined by the Organization. Access privileges will only be granted to the extent necessary to provide the Services and the Software and will not access or attempt to access any the Organization Information other than those required to provide the Services and the Software;

ii) provide each individual personnel of THRIVE Health who is permitted access to the Organization Systems or Information with a unique access ID and password;

iii) ensure that any access IDs, passwords or other access mechanisms, in each case relating to the Organization Systems (which will be deemed Confidential Information of the Organization) and Information will be used only by the personnel of THRIVE Health to whom they are issued and only for purposes of providing the Services and the Software, and access IDs are not shared among personnel of THRIVE Health;

iv) perform reviews, at least annually, of access entitlements for all THRIVE Health individuals with access to the Information;

v) remove any access to Information where no longer required (e.g., termination, change in role or responsibilities, etc.) in a timely manner, and in any case no longer than forty-eight (48) hours.

6. Security Incident Notification

a) If THRIVE Health has reason to suspect or becomes aware of a Security Incident, THRIVE Health will promptly:

i) notify the Organization in writing to a person designated by the Organization in writing to receive such notices of the Security Incident and in any event within twenty-four (24) hours after THRIVE Health first became aware of the Security Incident;
ii) execute reasonable measures to mitigate the effects, minimize all damage resulting from the Security Incident and to restore the Services; and
iii) adopt and employ measures to prevent the recurrence of the Security Incident and other security events of a similar nature or those which can be exploited through similar vulnerabilities.

b) THRIVE Health will provide the Organization with all information that the Organization may request, acting reasonably, about the root causes, the nature and the impact of the Security Incident, including:
i) information relating to the timing and duration of the Security Incident,
ii) dates of Security Incident occurrence, discovery, response, mitigation, and resolution,
iii) the identity of each Member or Authorized User affected by the Security Incident, the manner and extent to which each Member or Authorized User was affected were affected, and
iv) and other information reasonably required for THRIVE Health and for the Organization to meet their obligations under Applicable Laws.

c) If the Organization determines that THRIVE Health has not provided sufficient information for the Organization to meet its obligations under Applicable Laws, then, upon the Organization' written request, such additional information will be provided to the Organization.

d) For clarity and avoidance of doubt, THRIVE Health will immediately notify the Organization of any Security Incident occurring at the facilities, infrastructure or services controlled or provided by the Cloud Services providers as soon as THRIVE Health learns of such Security Incident. THRIVE Health will cooperate with the Organization and will provide the Organization with all information that THRIVE Health receives from the Cloud Services providers with respect to any such Security Incident.

e) THRIVE Health will coordinate with the Organization and take all reasonable measures requested by the Organization in the event of a Security Incident recognizing that the Organization may have its own notification obligations under applicable laws. Notwithstanding the foregoing, save for where THRIVE Health is required by any applicable law (in such cases, THRIVE Health will notify the Organization in writing and cooperate with the Organization to manage the notifications), THRIVE Health will not provide notice of Security Incidents to Members in respect of any the Information that is Personal Information as such notices will be provided by the Organization.

f) THRIVE Health will maintain an information security response program that enables THRIVE Health's security personnel to anticipate, prevent, be notified of and to respond to threatened, possible and actual Security Incidents on a continuous, twenty-four (24) hours, seven (7) days week basis (the "Security Monitoring Program"). The Security Monitoring Program will provide for: the internal report and management by THRIVE Health security personnel of threatened, possible and actual Security Incidents as fast as technically possible; and internal escalations of the threatened, possible and actual Security Incident to upper management of THRIVE Health so as to ensure that THRIVE Health will appropriately comply with its security obligations hereunder.

g) THRIVE Health will keep and maintain records of all Security Incidents (in accordance with the provisions of this Agreement and in accordance with applicable laws). Upon request of the Organization, THRIVE Health will promptly provide the Organization with access to, or a copy of, such records to the extent required for the Organization to meet its obligations under applicable laws.

Appendix B: Privacy Requirements

1. Introduction

a) This **Appendix B** set outs the standards governing the protection of Personal Information that THRIVE Health, the Software and the Services hereunder will comply with at all times.

b) Unless otherwise expressly provided hereunder, all Section references in this Schedule are references to Section numbers of this Schedule and not to Sections of other parts of this Agreement.

2. Definitions

a) In this **Appendix B.** the following capitalized terms and expressions have the following meanings: **"Security Incident"** has the meaning ascribed to it in **Appendix C - "Security Requirements.**

b) In this **Appendix B** and in **Appendix C. "Personal Information"** refers to Personal Information included in the Information and Member Information stored by THRIVE HEALTH on behalf of the Organization under this Agreement.

c) Capitalized terms and expressions not otherwise defined in this **Section 2** have the terms that are ascribed to them in the main body of the Agreement or, in the absence of definition within the main body of the Agreement, such capitalized terms and expressions will have the generally accepted industry or technical meaning given to them.

3. THRIVE Health's Privacy Obligations

THRIVE Health will:

a) only use, transfer, store, disclose or otherwise process Personal Information collected on behalf of the Organization under this Agreement to the extent necessary to fulfill its obligations under this Agreement or as otherwise permitted in the Agreement.

b) treat all Personal Information as confidential and it will limit access to Personal Information to those of its employees and subcontractors who have a need to access Personal Information to allow THRIVE Health to fulfill its obligations under this Agreement;

c) advise its employees and subcontractors receiving Personal Information of the obligations of THRIVE Health respecting confidentiality of Personal Information;

d) except as may be:

   i) otherwise expressly provided for in this Agreement;

   ii) required by applicable Privacy Laws;

   iii) required to provide the Services; or

   iv) receive payment for Fees set forth in this Agreement;

   not share or disclose Personal Information to any third party, unless the Organization has consented in writing to such disclosure or sharing. In all circumstances, where Personal Information is transferred to a third party, THRIVE Health will enter into a written agreement with the third party that requires the third party to comply with all of the terms of this Schedule and the Agreement with respect to Personal Information. THRIVE Health will remain fully responsible and liable for the use and transfer of any Personal Information that THRIVE Health transfers to any third party and for the actions and omissions of such third party in connection with the Personal Information disclosed to such third party;

e) establish, implement and maintain documented privacy policies and practices {"Privacy Compliance Program") governing the collection, use, disclosure and protection of Personal Information as required under applicable Privacy Laws and in line with industry standards;

f) permit representatives of the Organization to review THRIVE Health's Privacy Compliance Program (which will remain the Confidential Information of THRIVE Health), including the training of relevant personnel, as those policies and practices relate to Personal Information;

g) establish, implement and maintain adequate security measures to protect the security and confidentiality of Personal Information, including physical, technological and administrative measures. Such security measures will comply with, or be more stringent and protective than, the security requirements of **Appendix C - "Security Requirements":**

h) permit representatives of the Organization (including auditors appointed by the Organization) to review THRIVE Health's privacy practices and security measures and its processes in place for the disclosure, sharing, use of and access to Personal Information subject to this Agreement (which will remain the Confidential Information of THRIVE Health unless the Organization is required to disclose such Confidential Information under applicable laws);

i) provide the Organization with logs of any access, use or transfer upon request to support response to inquiries, complaints, requests for access or security incident investigations.

j) reasonably cooperate with the Organization in the Organization' privacy impact assessment and security impact assessment of the Software. Where any additional features or services are added to the Software with respect to the disclosure, sharing, use of and access to Personal Information subject to this Agreement, where required, THRIVE Health will complete a privacy impact assessment and security impact assessment in accordance with the Organization's applicable policies and processes prior to launch of such additional features or services;

k) not access or store any Personal Information outside the Territory (as defined in the main body of the Agreement. Other than the parties listed in THRIVE Health's Privacy Notice (Attached as Appendix E) and in Appendix C, THRIVE Health will not engage any third party to process Personal Information on its behalf and where consent is obtained from the Organization, THRIVE Health will conduct appropriate due diligence as regards that third party's privacy and security practices and THRIVE Health will obtain the written agreement of the third party to comply with provisions relating to the protection of Personal Information transferred to such third party that are substantially aligned with those of this Agreement.

l) unless expressly prohibited by Applicable Laws, immediately notify the Organization of any inquiries, complaints, or notices of investigation or non-compliance received from any Canadian or foreign governmental or regulatory authority or agency related to the collection, use or disclosure of Personal Information as part of the Software or the Services, and it will cooperate fully with the Organization in responding to any such inquiries, complaints or notices;

m) if THRIVE Health is required or becomes compelled by a legal, judicial, regulatory or administrative order to disclose any Personal Information relating to Members, the Organization will (unless expressly prohibited by applicable laws):

    i) promptly notify the Organization in writing of the legal, judicial, regulatory or administrative order compelling disclosure;

    ii) cooperate with the Organization in taking legally available steps to resist or limit the disclosure and to maintain confidentiality by the court or regulatory or administrative body; and

iii) where the Organization:

i. notified THRIVE Health in writing that it will not take legal steps to resist the disclosure; or

ii. was not successful in lawfully resisting or limiting the disclosure;

THRIVE Health will employ reasonable efforts to get the judicial or administrative body to keep the Personal Information confidential and will only disclose Personal Information that is clearly identified in the order compelling disclosure.

n) if it becomes aware of, or has reason to suspect, a breach of any of its obligations in this Appendix B, including any Security Incident related to Personal Information or any loss of, unauthorized access to, or unauthorized use or disclosure of, any Personal Information, it will comply with Section 7 of Appendix C - "Security Requirements".

o) THRIVE Health acknowledges that it is familiar with the requirements of the *Freedom of Information and Protection of Privacy Act* [RSBC 1996] CHAPTER 165 (FIPPA) governing Personal Information that are applicable to it as a service provider.

p) THRIVE Health must in relation to Personal Information comply with the requirements of FIPPA that are applicable to it as a service provider, including any applicable order of the commissioner under FIPPA.