CITF Data Access Agreement

This agreement ("Agreement") is entered into this Click or tap to enter a date. (the "**Effective Date**"), at Montreal, Quebec, Canada

BETWEEN

The Royal Institution for the Advancement of Learning/McGill University having a principal place of business at 845 Sherbrooke Street West, James Administration Building, Montréal, Québec, H3A 0G4 (**"McGill")**. McGill is the host institution for the COVID-19 Immunity Task Force **("CITF"**) Secretariat.

AND

INSERT: User Institution Name, with a main address at *INSERT: Address* **("Institution")**

AND

*INSERT: Name of Investigator***,** with researcher status at *INSERT: Institution Name*, with an office at *INSERT: Address (address, city, province/state, country, postal code)* **("Approved User")**

McGill, Institution and Approved User, are hereinafter called the "**Parties**", individually a "**Party**" and, Institution and Approved User collectively as "**Recipient**".

WHEREAS:

A. Dr. Timothy Evans (McGill) is the Executive Director of the CITF Secretariat hosted at McGill funded by the Public Health Agency of Canada on behalf of the Government of Canada to support the activities of the CITF to measure the scope of coronavirus infection in Canada and rapidly provide information to the Government of Canada needed to manage the COVID-19 pandemic;

B. Dr. David Buckeridge (McGill), is the Scientific Lead of Data Management at the CITF and oversees the data obligations under this Agreement;

C. The CITF Secretariat is mandated to coordinate multi-site sero-surveys assessing COVID-19 immunity in the Canadian population and to provide regular scientific updates to the Government of Canada on the state of serologic testing and the evolving understanding of immunity related to SARS-CoV-2 (CITF Study);

D. The CITF Study will include the creation of a database where data that is shared by consenting Public Health Agency of Canada and/or Canadian Institutes of Health Research funded studies will be centralized, harmonized and stored (CITF Database) in compliance with the CITF Guiding Principles and CITF Data Access Policy in Schedule A and following REB approvals. The CITF controlled access data (CITF Data) from the CITF Database will be securely made available to third-parties through this CITF Data Access Agreement for further research;

E. *INSERT: User Scientist's name* (the "Approved User") is a *INSERT: Position / Function*, at the Institution, where he/she carries or wishes to carry out a project entitled *INSERT: Title of Research Project*, for which access to CITF Data will be required;

F. Recipient agrees that the use and analysis of CITF Data and the publication of ensuing research results, will be performed in compliance with the terms of this Agreement and took note of their obligations under the CITF Data Access Policy and Guiding Principles as described in Schedule A is an integral part of this Agreement. All obligations contained therein are part of this Agreement;

G. The purpose of this Agreement is to allow the Recipient access, use, and to analyze CITF Data to perform research that advances knowledge on SARS-CoV-2 and related outcomes, and to publish the results.

The parties hereto agree as follows:

1. Definitions

Agreement: CITF Data Access Agreement.

CITF Data: CITF controlled access data that is described in the data access request form in Schedule B

DAC: CITF's Data Access Committee.

Project: Description of the intended use of the requested CITF Data in the data access request form in Schedule B.

Transferred Materials: CITF Data described in Schedule B that has been approved by DAC for transfer to the Recipient.

2. Data Security, Data Confidentiality and Accountability

2.1 Security measures specified in Schedule C will apply to all Transferred Materials. The Recipient undertakes to respect these security measures during the Project. The most up-to-date version of the CITF Data Security Policy is available at https://www.covid19immunitytaskforce.ca/wp-content/uploads/2022/11/data-security-policy-en.pdf. The Recipient is responsible for remaining aware of any changes made in the CITF Data Security Policy and ensuring continued compliance with said policy.

2.2 The Recipient shall agree to the audit of their data security and management documentation, and/or to undergo an independent audit of the physical, technological, and organisational security measures applied to their data. McGill can compel such audits to ensure the security and confidentiality of Transferred Materials. These audits may be conducted with reasonable prior notice. Any discrepancies between the security measures specified in Schedule C and what is found at the Recipient research facility will have to be corrected within sixty (60) days of notice by McGill. The audits are conducted at McGill expense.

2.3 Confidentiality of the Transferred Materials will be maintained at all times. Transferred Materials, including any copies thereof, may only be used for the Project as described in Schedule B, and may not be disclosed, or transmitted to anyone except employees working directly with the Recipient and co-investigators including co-applicants or other personnel from other institution(s), indicated in the Schedule B who will require direct access to the Transferred Materials and who agree to be bound by the terms of this Agreement. The Recipient shall retain control of the Transferred Materials at all times. It is the responsibility of the Recipient to inform the staff and co-investigators, including co-applicants and other personnel at other third-party institution(s) entering into contact with the Transferred Materials of the obligations contained in Schedule A and this Agreement. As such other parties, including research collaborators, are required to complete a Schedule B and CITF Data Access Agreement. Such parties must subsequently receive the necessary approvals from the DAC to access and use the Transferred Materials. Data access will only be provided to institutional email addresses. The following exceptions apply where transfer or disclosure may occur for Transferred Materials: 1.) as required by national audits or as otherwise required by law; and 2.) as required for third-party service providers retained by the Recipient to carry out services under the Project in compliance with the terms of the CITF Data Security Policy as described in Schedule C.

2.4 The Recipient agrees to respect the strict confidentiality of the Transferred Material and all applicable laws, regulations, guidelines and policies (including, but not limited to laws regarding the privacy or protection of personal or medical information and the Quebec Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information) relating to the protection of the Transferred Materials. Furthermore, the Recipient shall ensure that all persons working under the Approved User on the Project have committed to do the same.

2.5 The Recipient agrees to provide to the CITF an updated Project description prior to making any changes to their Project that affect the use of the Transferred Materials. Such information must be provided by submitting an updated Schedule B to the CITF data access request portal.

2.6 The Recipient agrees to provide to the CITF an updated list of names of the Principal Investigator, Authorized Personnel, and Authorized Students as described in Schedule B that can access the Transferred Materials within thirty (30) days of any changes occurring. This requirement arises if the Principal Investigator, or any Authorized Personnel or Authorized Students depart from the Project. Such information must be provided by submitting an updated Schedule B to the CITF data access request portal.

3. Fees. The Institution shall pay to McGill the access fees specified in Schedule D attached hereto within forty-five (45) days after receipt of the invoice or note waiver if applicable.

4. Research Ethics Approval, Representations and Warranties.

4.1 The Recipient confirms that all necessary research ethics approvals and other approvals required to perform the Project as described in Schedule B have been obtained and they will continue to hold such approvals for the duration of the Project.

4.2 The Recipient confirms that a copy of the research ethics approval(s) has been provided to McGill to perform the Project and the research ethics approval(s) are appended to Schedule B.

4.3 All documents in Recipient's possession concerning ethical approval of the Project, including any subsequent amendments/renewals that may be applicable, have been provided to McGill. If the Institution does not require research ethics approval to perform the intended Project, this note will be included in Schedule B.

4.4 The Recipient confirms that they have read and understand their obligations under the CITF Data Access Policy and CITF Guiding Principles in Schedule A and will use the Transferred Materials in accordance with all applicable laws.

5. Harm, Discrimination, and Re-identification. Re-identification can occur if data is combined with other sources of data to produce new information, including other sources of health information or data that is accessible in public sources such as social media websites. The Recipient agrees to the following:

5.1.1. To not use the Transferred Materials in a manner that could cause harm to or discriminate against individuals, especially the persons to whom the Transferred Materials relates, their families, and their communities.

5.1.2. To not to use the Transferred Materials to attempt the re-identification of the persons to whom the Transferred Materials relates, their families, and their communities.

5.1.3. To not use the Transferred Materials for any purposes, research or other, that pose a reasonably foreseeable risk of causing the re-identification of the persons to whom the Transferred Materials relates, their families, or their communities.

5.2 If the Recipient intentionally, inadvertently, or by the act of an agent or related third party, cause the re-identification of a person to whom the Transferred Materials relates, or have reason to believe the re-identification of a person to whom the Transferred Materials relates. The CITF with be immediately notified and assistance will be provided to the CITF to comply with any measures required by the CITF to mitigate or respond to any material or anticipated consequences occasioned by such re-identification.

6. Property of Transferred Materials. Nothing in this Agreement will operate to transfer any property rights in the Transferred Material.

7. Exclusive Access: No exclusive access will be granted to any portion of the Transferred Materials. McGill may grant access to the Transferred Materials to others and may use it for its own internal purposes.

8. Data Breach Notifications and Procedures. The Recipient agrees that immediate notice will be given to the CITF of any data breach known to have affected the Transferred Materials or that it is reasonable to assume may have affected Transferred Materials. The Recipient further agrees that they will comply with any measures required by the CITF to mitigate or respond to any material or anticipated consequences occasioned by such Transferred Materials breach. The Recipient acknowledges that the CITF may provide notice of such data breach to data contributors, authorities, and institutions. The CITF may further provide notice of such data breach to individuals affected by or thought to be affected by the data breach. The CITF is not required to inform the Recipient that it has provided notice of data breach to third parties**.**

9. Scientific Publications and Acknowledgment Requirements. The Recipient will be required to comply with the CITF Publication Policy as described in Schedule A. The Recipient agrees to the following: 1.) Maintaining the confidentiality of the Transferred Materials in all reports, publications and presentations resulting from the use of the Transferred Materials. There will be no publishing of any Transferred Materials or any research outputs, such as derived data that can be potentially identifying. 2.) Remaining aware of any changes made to the CITF Publication Policy and ensuring continued application with said policy. 3.) To follow the Fort Lauderdale Guidelines, the Toronto Statement, as well as the GA4GH Framework for Responsible Sharing of Genomic and Health-Related Data. This includes but is not limited to recognizing the contribution of the CITF and including a proper acknowledgement in all reports or publications resulting from the use of Transferred Materials. Such acknowledgement shall include the following language: "*This project was supported by funding from the Government of Canada, through the COVID-19 Immunity Task Force./ Ce projet a été soutenu par un financement du Gouvernement du Canada, par le biais du Secrétariat du groupe de travail sur l'immunité COVID-19* ". The Recipient will also need to acknowledge the CITF in publications, where the acknowledgment could be a link to a dynamic list of studies contributing data to the CITF, or by citing a central marker paper describing the work and authored by individuals from the CITF Secretariat and principal investigators that shared their study data with the CITF to include in the CITF Database. .

10. Reporting Obligations: The Recipient shall comply with the following reporting obligations: i) **notify** McGill without delay for: a) incidents affecting the confidentiality of participants; b) incidents affecting the security or integrity of data/samples; c) suspension or lapse of any relevant authorizations (e.g. Ethics approval), professional qualifications, funding or approvals. Significant modifications to the approved project/protocol (including additional researchers or staff who will be accessing the data) or its timeline will require the submission of an updated Schedule B to data@covid19immunitytaskforce.ca

11. Undertakings and Liability. The Institution assume all liability or damages arising from the use, storage or disposal of the Transferred Materials and further agrees to defend, indemnify and hold harmless McGill and its agents and employees from all liabilities, damages, demands, expenses and losses arising out of the acceptance, use for any purpose, handling or storage and/or disposal of the Transferred Materials and in respect of all matters associated with the research results arising from the use of the Transferred Materials by the Recipient.

12. Default of Approved User or Institution. Failure to comply with the terms of this Agreement may result, in addition to termination of this Agreement pursuant to Section 13.1, in the disqualification of the Approved User or the Institution (or both) from receiving any additional data from McGill. McGill reserves the right to institute and to take appropriate proceedings at law (or in equity, where applicable) against the Approved User or the Institution (or both) in connection with breaches of this Agreement.

13. Termination

13.1 This Agreement will terminate the earlier of 2 years after its Effective Date or at the time that the research ethics approval applicable at the time of application ceases to be applicable (where relevant), unless the Parties agree in writing to renew it. Upon termination of the Agreement, the Approved User will stop using and destroy the Transferred Materials in Approved User's possession. If applicable, the Recipient will be permitted to archive the Transferred Materials upon request and approval from McGill for the period of time required for peer review and audit purposes but not to exceed 1 year following the termination of this Agreement. Once this period of time has elapsed, the Recipient undertakes to destroy all Transferred Materials and all copies thereof in Recipient's possession. When requested by McGill, the Recipient shall certify in writing that the Transferred Material and all copies thereof were destroyed

13.2 The Approved User and Institution agree that McGill may terminate this Agreement if the Approved User or the Institution (or both) are in default of any of the provisions of this Agreement and this default has not been remedied within sixty (60) days of written notice sent by McGill to the Approved User or the Institution in respect of this default. Upon termination of this Agreement pursuant to this Section 13.2, the Approved User will return all Transferred Materials in his or her possession to McGill or destroy them and all copies thereof in possession of the Approved User or the Institution according to the instructions provided by McGill. The Approved User and Institution will provide McGill with a certificate attesting to such destruction. In the event the Approved User is found to be in breach of this Agreement and such breach

has not been remedied in accordance with this Section 13.2, the Approved User will not be entitled to publish the results of any Project except with the written agreement of McGill.

14. No Warranties. The Transferred Materials accessed or delivered pursuant to this Agreement are understood to be experimental in nature and are provided "as is". McGill makes no guarantees, no express or implied warranties of merchantability, utility, efficacy, safety, identity, composition, and accuracy or fitness for a particular purpose or that the use thereof will not infringe any patent and there is no guarantee that the Transferred Materials is free of third-party intellectual property rights, database rights, or other related rights

15. Intellectual Property Claims and Licensing Guidelines.

15.1 The Recipient agrees that they will not make any claims on the Transferred Materials or CITF Data as described in Schedule B that includes intellectual property, database rights, or related rights.

15.2 The Recipient agrees that they will not use intellectual property protection, database rights, or related rights in a way that would prevent or block access to, or use of, any element of the Transferred Materials or CITF data, or research conclusions derived from the Transferred Materials or CITF data.

15.3 The Recipient may perform further research that may add intellectual and resource capital to the Transferred Materials, and decide to obtain intellectual property rights on these downstream discoveries. The Recipient agrees with respect to any further research that would add intellectual and resource capital to the Transferred Materials, to follow the Fort Lauderdale Guidelines, the Toronto Statement, as well as the GA4GH Framework for Responsible Sharing of Genomic and Health-Related Data, and to implement licensing policies that will not obstruct further research.

16. Notices. Any notice to be given by a Party shall be sent to the following:

McGill: CITF Management	**McGill: Legal Matters:**
David Buckeridge Scientific Lead, Data Management and Analysis Email: david.buckeridge@mcgill.ca	McGill University Office of Sponsored Research James Administration Building 845 Sherbrooke W., 2nd floor Montreal Quebec, H3A 0G4 Attn: Carole Goutorbe Director Email: carole.goutorbe@mcgill.ca
If for Approved User: Approved User Contact: (Name, Title, Email)	If for Institution (add contact details) Institution Contact: (Institution name, Office address, Contact person, Email)

17. General Provisions

17.1 This Agreement and the attached Schedules represent the entire understanding between the Parties related to the Transferred Materials and the Project and supersedes any previous understandings, commitments or agreements, whether written or oral. If any provision of this Agreement is wholly or partially unenforceable for any reason, all other provisions will continue in full force and effect.

17.2 This Agreement is governed by and will be construed in accordance with the laws of the Province of Quebec and the applicable laws of Canada.

17.2.1. In the event of a dispute, conflict, controversy, contestation, claim or other form of dispute ("Dispute"), the Parties agree to meet without delay, to negotiate in good faith and to use their best efforts to try to resolve such Dispute within thirty (30) days. The Parties agree that their respective leaders shall actively participate in this negotiation process.

17.2.2. In the event of the failure of these negotiations, the Parties may choose to appear at least once before a professional mediator duly authorized to assist in the resolution of Disputes.

17.2.3. In the event of failure, the dispute arising hereunder shall be submitted to the exclusive jurisdiction of the provincial courts of Quebec, in the judicial district of Montreal.

17.3 The following provisions will survive termination of this Agreement: 5, 9, 10, 11, 12, 13, 15, 16 and 17.

17.4 The headings contained in this Agreement are for convenience and reference only and shall not define or limit the scope, or affect the interpretation of, its provisions.

17.5 This Agreement shall not be amended, modified, varied, or supplemented except in writing signed by each of the parties.

17.6 No Parties shall use, or authorize others to use, the name, symbols, or marks of another Party hereto or its staff for any endorsement purposes without prior written approval from the Party whose name, symbols or marks are to be used.

17.7 No Parties may assign any of its rights or obligations under this Agreement without the prior written consent of the other Parties.

17.8 Language. *Les Parties ont requis que cette entente soit rédigée en anglais.* The Parties have requested that this Agreement be drafted in English.

17.9 Nothing in this Agreement creates, implies, or evidences any partnership or joint venture between the Parties, or the relationship between them of principal and agent. No Parties shall have the authority to act on behalf of any other party or to bind another party in any manner.

17.10 Each Party confirms that it is permitted to enter into this Agreement; to consent to its conditions and that each has authority to sign this Agreement. This Agreement may be executed in counterparts and may be executed and delivered by facsimile or electronically by PDF and all such counterparts, facsimiles and PDF copies shall together constitute one Agreement. The Parties agree that facsimile or PDF copies of signatures have the same effect as original signatures.

IN WITNESS WHERE OF McGill and Recipient have caused this Agreement to be executed in duplicate by their respective duly authorized representatives.

The Royal Institution for the Advancement of Learning/McGill University

Signature

Name: Carole Goutorbe

Title: Director, Office of Sponsored Research

Date: Click or tap to enter a date.

The Institution

Signature

Name: Name

Title: Title

Date: Click or tap to enter a date.

Signature

Name: Name

Title: Title

Date: Click or tap to enter a date.

Approved User

Signature

Name: Name

Title: Title

Date: Click or tap to enter a date.

Signature

Name: Name

Title: Title

Date: Click or tap to enter a date.

Acknowledgment by Scientific Lead Data Management, CITF to McGill University

I, Dr. David Buckeridge, having read and understood this Agreement, hereby agree to act in accordance with all the terms and conditions herein and further agree to ensure that all CITF participants are informed of their obligations under said terms and conditions.

Signature

Schedule A:
CITF Data Access Policy and Guiding Principles:

1. CITF Introduction

The COVID-19 Immunity Task Force (CITF) was created in late April 2020 with the goal of catalyzing, supporting, and harmonizing research into COVID-19 immunity to inform Canadian policymakers, allowing them to make evidence-based decisions.
The CITF has supported numerous studies that aimed to:

- Determine the extent of SARS-CoV-2 infection and vaccination in the general Canadian population and in specific communities and priority populations;
- Understand the nature of immunity arising from SARS-CoV-2 infection;
- Develop improved antibody testing methods;
- Monitor the effectiveness and safety of vaccines as they are rolled out across Canada and in specific sub-groups of the population such as children;
- Determine the need for, and optimal timing of, booster shots;
- Develop models of population immunity to guide public health efforts as the pandemic evolves; and,
- Explore cross-cutting themes.

The CITF was mandated by the Government of Canada to establish and oversee a Secretariat coordinating multi-site sero-surveys assessing COVID-19 Immunity in the Canadian population. The Secretariat has supported researchers in many ways, including:

a. Coordinating testing to detect COVID-19 antibodies, viral material, and cellular immune response;
b. Standardizing the data collected across studies through questionnaires about personal characteristics, COVID-19 infection history, and lifestyle;
c. Facilitating investigators in obtaining consent to permit the sharing of clinical and biological test results and other study data for the purpose of secondary research; and,
d. Working with researchers and their institutions to allow study data to be deposited in the CITF Databank to enable further research using those data.

2. Guiding Principles

The COVID-19 Immunity Task Force embraces the following principles and practices:

a. Partner in all of its work with the Government of Canada and provincial/territorial governments and their agencies, as well as the research community, public health and healthcare professionals/institutions, and a range of community groups.
b. Identify priority issues related to serologic testing and its application, paying close attention to diverse needs for information across the country.
c. Establish an ethos in which the rigorous gathering and rapid sharing of data to inform Canadians and to advance the broad public interest over-rides any considerations of personal/group advancement.
d. Mobilize the best science and study designs that are responsive to the rapidly evolving state of the science related to COVID-19 immunity.
e. Establish fair and transparent processes consistent with principles of equity, diversity, and inclusion (EDI) that offer all interested partners across the country an opportunity to participate in the CITF, while appropriately managing conflicts of interest.

f. Work with partners to ensure protection of privacy in data-gathering and safe handling of any and all biological samples.
g. Collaborate with partners and use existing data- and sample-gathering capacity wherever possible to enhance cost-efficiencies and avoid unnecessary duplication.
h. Provide a central coordination for the Task Force within a Secretariat that facilitates rapid development of studies, their effective implementation, and rapid reporting of results to key audiences, including decision makers and interested stakeholders, and the broad Canadian public.
i. Promote ethical and sound participatory practices that engage relevant stakeholders from study design through to dissemination and application of findings.
j. Adhere to best practices regarding any authorship of scientific publications eventually arising from this work, while ensuring that all participants understand that this work is in the public interest, requiring rapid dissemination of reliable and relevant results.
k. Liaise with relevant entities in other countries and with international agencies involved in serologic surveys and studies to understand immunity related to SARS-CoV-2.
l. Communicate the leadership, membership, activities and results of the Task Force with openness and transparency.

3. Definitions

Access: To retrieve, consult, copy, or process a digital, conceptual, or physical asset (including a dataset), in whole or in part.

Access Applicant: Researcher applying for Access to CITF Data following the Controlled Access Procedure. All applicants must be affiliated with an institution (public or private) and are accepted internationally.

Approved Institution: Institution under which the approved Access Applicant is conducting the Research project.

Access Policy: Policy governing the requirements and procedures to Access CITF Data. To be used in conjunction with the terms outlined in the CITF Access Agreement.

Approved Research Project: Research project being conducted by the Access Applicant which must be reviewed for compliance with Access Policy requirements and CITF Guiding Principles by the Data Access Committee.

CITF Access Agreement: A signed agreement between the Approved Applicant, Approved Institution and McGill University that sets out the terms and conditions in the CITF Access Agreement that allows Access to the requested CITF Data.

CITF Controlled Access Procedure: The process by which researchers can gain Access to individual records contained in the CITF Database. This procedure is in conjunction with the Access Policy and is implemented by the Data Access Office, Data Access Committee and CITF Data Team. It consists of Access Application submission, Access Application validation, Access Application acceptance or rejection, and data acquisition.

CITF Data: Coded study data collected from research participants by researchers at local study sites, including survey data and sample data from relevant collections and cohorts.

All CITF Data are coded at the local study site before being deposited in the CITF Database. Coding means that the researchers at the local study site replace all direct identifiers, such as name and civic address, by a code that is unique to each study participant. Individual-level, coded data is housed in the CITF Database and is made available to researchers through the CITF Controlled Access Procedure.

CITF Database: The technological platform that holds the CITF Data. This refers to the physical infrastructure used to host the data, the informational networks that contain the data, and the organizational and professional activities that maintain and direct the functioning thereof.

Core Data Elements: A list of mandatory data elements and data formats that should be included in all datasets provided to the CITF for inclusion in the CITF Database. These make up the CITF Harmonized Data.

CITF Data Team: Team within the CITF Secretariat who specialize in data analysis, curation and management. They are responsible for maintaining the CITF Database and preparing datasets for approved Access Applicants.

Data Access Application: Form submitted through the CITF Data Access Portal to the Data Access Office by the Access Applicant to request Access to CITF Data that requires contact information of the Access Applicant and affiliated institution, research project information and proof of REB approval.

Data Access Committee: Committee with varying areas of expertise that have been assembled to review and make decisions concerning the viability of Data Access Applications. Its composition and responsibilities are outlined in the Data Access Committee Terms of Reference.

Data Access Office: Individual who communicates with Access Applicants, manages and keeps records all Data Access Applications, performs validation of Access Applications and prepares them for Data Access Committee review.

Data Access Portal: Online portal, powered by Maelstrom Research, to which Access Applicants may create an account, explore CITF Data and submit a Data Access Application.

Harmonized Data: The centralized dataset containing the Core Data Elements from all CITF approved studies. CITF Data are harmonized to ensure consistency across studies. Harmonized Data are still considered CITF Data and must be Accessed through CITF Controlled Access Procedure.

4. Access Policy

4.1 Objectives

The CITF Database receives data from CITF-funded studies, including cross-sectional studies and longitudinal cohort studies, as well as the research data of external researchers. Once study data are received, the CITF Data Team works to create a dataset which harmonizes the Core Data Elements collected from all studies. The Harmonized Data in the CITF Database will be made available to researchers in Canada and internationally who request Access to the data following the CITF Controlled Access Procedures.

The CITF Database aims to increase the impact of Canadian Covid-19 research studies. In harmonizing and making these data accessible, the Task Force hopes to provide the research community with a means to Access a wide variety of Covid-19 data in a common format, thus removing important barriers to Access.

4.2 Scope

This Policy includes the requirements and processes by which researchers may Access data stored in the CITF Database. These individual-level (de-identified) data include survey data, individual-level laboratory test results and other baseline health data that the CITF Data Team has harmonized. These data can be Accessed by researchers upon approval of a Data Access Application by the CITF Data Access Office and CITF Data Access Committee.

The list of Core Data Elements, non-core data elements, and metadata fields available for each study dataset are openly available for consultation. Non-core data elements will not be hosted in the CITF Database and the CITF will not be responsible for ensuring Access to these data, nor will the CITF provide any assurances with regard to the accuracy or quality thereof, its fitness for a particular purpose, or the rights and permissions inherent therein.

5. Access Limitations

The data stored in the CITF Database will be available for access to any researcher affiliated with a public or private institution, including institutions outside of Canada. Requests to Access data in the CITF Database may be rejected by the Data Access Committee or deemed invalid by the Data Access Office should the scientific research objectives not follow the CITF guiding principles, or if insufficient information or documentation is given. Access to CITF Data is limited to the Access Applicant and research staff who have been declared as data users in the Data Access Application and CITF Access Agreement, all of whom are bound by the terms and conditions in the CITF Access Agreement. Should updates be made to the research team, an Amendment form must be submitted with the relevant changes to the Data Access Office and Data Access Committee for review.

6. Privacy of Participants

In order to ensure the security of the CITF Data and the protection of the privacy of individual participants for whom data has been collected, all approved users declared on the Data Access Application and CITF Access Agreement must comply with the data security policy (Schedule C – CITF Data Security Policy).

7. Indigenous Data Governance

The CITF recognizes the historic inequitable and harmful nature of research involving Indigenous Peoples and their communities. In addition, the CITF recognizes that in facilitating the sharing of data with researchers, some manipulations and interpretations of the data could have implications for Indigenous Peoples and communities. As such, this document provides a set of principles, which the CITF will use to protect Data Assets.

Currently, the CITF does not intend to centralize data from any studies that focus exclusively on Indigenous Peoples and communities. The following principles therefore apply to CITF-funded studies from across Canada where some participants self-identify as an Indigenous Person or living in and Indigenous community.

As Indigenous Peoples and communities assert the right to govern how their information is used, controlled and disclosed, the OCAP principles are reflected in all applicable agreements, policies and procedures that concern Indigenous Data Assets. As such, researchers wishing to access the data must also comply with these policies. The following policies are actively being implemented:

The full set of principles and policies can be found in the *Governance of Data about Indigenous Peoples and Communities* document.

The CITF recognizes that some of the Core Data Elements could be analyzed in a manner that would risk the identification or stigmatization of Indigenous communities, including harmful psychological, social or other effects on communities or individuals. To limit this risk, Access Applicants are required to provide justification and evidence of REB approval when they request access to the following variables:

- Indigenous identity
- Living on Reserve
- Ethnicity of participant
- Rural FSA
- Postal Code

An expert in Indigenous health research has been appointed as a Data Access Committee Member. They will help to ensure appropriate Indigenous Data Governance when decisions are being made concerning access to data that involves the variables flagged above.

Moreover, if the requested data would allow the identification of communities, the Access Applicant must use appropriate engagement and procedures as dictated by the implicated communities.

8. Access Documents

8.1 Access Application Form

To Access CITF Data, an applicant must register for an account with the CITF Data Access Portal. A single member of the Access Applicant team is responsible for this account. They must then complete and submit the Data Access Application. Documentation to be submitted along with the application includes:

- Research Summary including justification for the requested variables and statistical analyses to be conducted
- Evidence of approval by a Research Ethics board for the research project or confirmation and justification for why REB approval is not required
- CV of the Researcher applying
- This Access Application will be validated for completeness and conformity by the Data Access Office and reviewed by the Data Access Committee.

8.2 Signed Access Agreement

Once approved by the Data Access Committee, the data requested from the CITF will be shared with the Approved User and their affiliated institution following completion of the Access Agreement with the Approved User, and signature of the agreement by the Approved Institution and McGill University.

9. Application Review Process

Access Applicants must create an account on the CITF Data Access Portal, where they will be able to explore data variables and submit Data Access Applications. The Access Application form is completed by the Access Applicant of the Research Project and must include all supporting documentation. Once submitted, the Access Application is validated by the Data Access Office for completeness and conformity. If necessary, the Access Applicant will be instructed by the Data Access Office to make changes. The Data Access Committee will review each Access Application according to the Criteria for Approval. An Access Application can be Approved, Rejected or Conditionally Approved. Access Applicants can revise their Access Application according to the comments received from the Data Access Committee, if applicable. Once approved, the Access Agreement is signed by all parties. The Data Management team proceeds with data preparation and processing steps in order to initiate data sharing with the Approved Institution.

Once data sharing has commenced, if there are any changes to the research project or research project personnel from the original Data Access Application that could affect the use of the CITF Data, an Amendment form must be completed by the Applicant, validated, reviewed and approved by the CITF Data Office and CITF Data Access Committee before changes can be carried out by the research team. Should a data breach occur that is known or, with reason, assumed to have affected the CITF Data, immediate notice must be given to the CITF and the CITF data security policy should be followed. Access Applicants accessing the data must also comply with the CITF Publication Policy when publishing research using CITF Data.

10. Criteria for Approval

The following criteria will be used by the Data Access Committee in considering whether to approve requests to Access CITF Data:

- Data Access Office has received all necessary documents.
- Data Access Office confirms availability of CITF Data
- Research is in accordance with the guiding principles of the CITF
- Research has been deemed scientifically sound and the project scope is appropriate
- Justification for the need of the CITF Data is provided
- Proof of REB approval, or justification for REB exemption, has been given
- Should CDEs (Core Data Elements) referenced as “sensitive” be requested, specific justification and study team expertise for the use of these variables is provided in the REB Approval and the Study Protocol.

11. Confidentiality of Applications

All information submitted in the Access Application Form will be kept confidential within the Data Access Office and Data Access Committee. Once Access is granted, general information about the Research Team and the associated Research Project will appear on the CITF Data Access "Approved Projects" Webpage for public view.

12. Publication Policy

Researchers Accessing the data must also comply with the CITF Publication Policy when publishing research using CITF Data.

- Maintaining the confidentiality of the CITF Data in all reports, publications and presentations resulting from the use of the CITF Data. There will be no publishing of any CITF Data or any research outputs, such as derived data that can be potentially identifying.
- Remaining aware of any changes made to the CITF Publication Policy and ensuring continued application with said policy.
- Following the Fort Lauderdale Guidelines, the Toronto Statement, as well as the GA4GH Framework for Responsible Sharing of Genomic and Health-Related Data.
- Recognizing the contribution of the CITF and including an acknowledgement in all reports or publications resulting from the use of data held in the Controlled Access Tier of the CITF Database. The following attribution should be used: The data used in this research was made available by the COVID-19 Immunity Task Force.
- Citing in all publications using data from the CITF Databank a central marker paper describing the work by the CITF Secretariat and Principal Investigators of studies that have deposited data in the CITF Databank.

13. Destruction of Data

Researchers agree to destroy their copy of the CITF Data on or before the date in their CITF Access Agreement. Researchers agree to maintain documentation evidencing the destruction of the CITF Data and to make such records available to the CITF on request.

14. Amendment to Applications

The approved user must inform the Access Office of any changes in the research project, or in the status of approved users or Approved Institution. Should changes to the research project personnel occur that could affect the use of the CITF Data, an Amendment form must be filled out with said changes. This change must be approved by the Access Office and Access Committee and new members must enter into the Access Agreement with McGill university.
In addition, should changes be made to the research project protocol or events occur during the project that could affect the use of the CITF Data, or the original information provided in the Access Application form, an Amendment form must be completed and approved. If the changes are minor or administrative, the form will be reviewed and approved by the Data Access Office. Should the changes be substantial, the data Access Committee will be required to conduct a full review. However, any suspected threats to the confidentiality and security of the CITF Data must be reported to the CITF and the Data security policy must be followed.

15. Return of Research Results and Incidental Findings

It will not be possible for the CITF nor Access Applicants to return research results of incidental findings to research participants. General information regarding the scientific research performed and the outcomes thereof will be made available on the CITF website. Information about the use of data in the CITF Database will also be made available in the academic publications of CITF researchers and of Access Applicant having Accessed data in the CITF Database.

16. Intellectual Property and Related Rights

Intellectual property rights, sui generis database rights, and related rights cannot be claimed on the CITF Data by parties other than the CITF. Intellectual property, sui generis database rights, and related rights claimed on the CITF Derived Data should not impede the use of primary CITF Data by the CITF, nor by researchers and other persons authorized to Access and/or use the CITF Data.

The CITF commits to invoking intellectual property rights, sui generis database rights, and related rights only for the purpose of safeguarding the Access of data contributors, the CITF, and other authorized parties to the CITF Data and associated resources. Patent protection will not be sought by the CITF for any innovations, such as functional assays or scientific approaches it creates. The CITF believes that Open Science delivers the most rapid and accessible scientific results for research participants. Nonetheless, it remains possible for data contributors or External Researchers to claim intellectual property protection on the innovations they create or the Derived Data they generate.

17. Derived Data

The CITF does not enforce any routine requirements to share derived data. However, if a researcher creates a variable that could be useful to others, the CITF will consider incorporating this into the CITF Database on a case-by-case basis.

18. Financial Considerations

There is currently no charge for researchers to Access.

Schedule B – CITF Data Request Form

Schedule C – CITF Data Security Policy

1. **Encryption and Password Protection.** Researchers agree that the CITF Data will be stored primarily on password-protected desktop computers or servers. If stored on mobile devices, such as laptop computers or remote storage devices, the CITF Data will remain encrypted when at rest.
2. **Physical Safeguards.** Researchers agree to keep desktop computers and servers holding the CITF Data in private rooms that can be locked and to lock the doors thereof if the researchers are not on site to monitor the use of the CITF Data.
3. **Data Safeguards.** Researchers agree to use a recognized virus and malware protection software on the desktop computers, laptop computers or remote storage devices (provided these can be outfitted with such protection) that will host the CITF Data.
4. **Organizational Safeguards.** Researchers agree to implement and adhere to organizational practices that enhance data security. Access to data must be limited to authorized personnel. Authorized personnel must remain demonstrably accountable to institutional leadership and senior personnel, as well as to the institution itself.
5. **Data Destruction.** Researchers agree to destroy the CITF Data at the time determined in the Data Request Form or equivalent document. Researchers agree to use an auditable method of data destruction to destroy the CITF Data. Researchers agree to maintain documentation evidencing the destruction of the CITF Data and to make such records available to the CITF on request.
6. **Training.** Researchers agree to ensure that the principal investigator, authorized personnel, authorized students and other persons at their institution that access the CITF Data are provided with training that addresses data security and data privacy, to a degree that is appropriate to their role and responsibilities.
7. **Record-keeping.** Researchers agree to maintain records of who has access to the CITF Data under their control or in their possession. Researchers agree to record the time interval and scope of data elements accessible to each approved user. Records must also be maintained detailing data destruction.
8. **Monitoring and Audit.** Records regarding CITF Data access and destruction shall be stored using technological means that allow for audit internally and by external researchers. Audits of user activity shall be conducted on a regular basis and shall be conducted immediately when irregular user activity occurs.
9. **Data Breaches.** Researchers shall use industry-standard technological mechanisms appropriate to protect health data to prevent data breaches, and that allow for data breaches to be detected. If a data breach occurs that is known or suspected to affect CITF Data, the CITF must be informed immediately and all known information about the data breach must be provided to them.
10. **Vulnerability Management**. Researchers agree to immediately take measures to patch and/or remediate all software and other security vulnerabilities that are discovered which could affect the CITF Data. Researchers agree to have policies in place to ensure the prompt and ongoing patching of vulnerabilities and to implement that policy effectively.
11. **Third Party Service Providers**. Researchers agree to use all contractual and other measures necessary to ensure that Third Party Service Providers comply with the terms of this Policy and are demonstrably held accountable to the CITF.

12. **Cloud Storage and Cloud Computing**. Researchers agree to adopt all contractual and other measures necessary to ensure that all Cloud Storage and Cloud Computing providers that will use or access the CITF Data remain accountable to them and to the CITF. These measures shall include, but not be limited to, providing specific details as to, and guaranteeing the auditability of: the jurisdictions of storage of the CITF Data, data retention and destruction practices, segregation of the CITF Data from other data, implementation of appropriate security measures, maintenance of adequate access logs, and adoption of appropriate procedures for resisting compelled access to the CITF Data.

Schedule D – Fees

Fees in accordance with this Project and article 4 have been set at **Fee waived** and must be paid 30-45 days after receipt of an invoice that will be sent to the primary user.