BrightHive Data Trust Agreement

Data Trust Legal Agreement

true

Last updated: Apr 13, 2020 at 09:15 AM

Contents

Data Trust Agreement

vC0.01.16 2020

BrightHive Data Trust

This Data Trust Agreement (the "Agreement") is entered into on **April 13, 2020** ("Effective Date") by and between the members as listed in the table below ("Members"), and Technical Trustee ("Trustee"), on behalf of the BrightHive Data Trust ("Data Trust"). Members, Data Trust, Trustee Affiliate, and Trustee may each individually be referred to herein as a "Party" and collectively as the "Parties".

Data Trust Members

Member 1

Member 2

Member 3

Member 4

Chapter 1

Recitals

WHEREAS, the Trustee acts on behalf of all Data Trust Members to support the creation and ongoing maintenance of the Data Trust. WHEREAS, Members may contribute data, including protected health data, personally identifiable data, or other protected data to the Data Trust.

WHEREAS, Members may access and use data resulting from the combination of one or more Members' contributed data, as allowable by state or federal law.

WHEREAS, Trustee and Members desire to establish a Data Trust for the purposes of ethically and sustainably sharing data in order to increase understanding of the populations served by Trustee and Members, improve services provided by Trustee and Members to populations served, identify new services needed by populations served, and/or otherwise improve societal outcomes for the populations served.

NOW, THEREFORE, in consideration of the premises and mutual covenants herein contained, the Parties hereto hereby agree as follows:

Chapter 2

Definitions

In this agreement:

- **"Aggregate Data"** shall mean information whose values have been generated by performing a calculation across all individual units as a whole. For example, while uncovering new treatment strategies, medical researchers might look for patterns in aggregated patient data, but have no way to identify specific individuals.
- **"Confidential Information"** shall mean non-personal information that holds value and importance for organizations, such as business plans and proprietary research or other intellectual property. The disclosure or loss of such confidential information can have potential negative impact on organizations, but it does not constitute a privacy breach because it does not involve the handling of personal information. Confidential Information does not include information which is (i) known by the Trustee or other Trust members prior to disclosure to them; (ii) generally available to the public other than as a result of breach of this Agreement; (iii) made available to the Trustee or other Trust members by any independent third party who has the right to disclose the information; (iv) information that is published; (v) is independently developed by the Trustee or other Trust members (vi) is required to be disclosed by a court of competent jurisdiction, law, or government rule or regulation.
- **"Data Access Levels"** shall mean the type of data a Data Trust Member and/or approved User may access, such as personal data, raw data. Access Levels shall be defined by the Governance Board and documented in Exhibit F attached hereto.
- **"Data Trust"** shall mean the Trustee, Member, and other Members which collectively form the Data Trust ("Data Trust") as constituted in the Data Trust Member Agreement.

- **"Data Trust Governance Board"** shall mean the decision-making body, consisting of at a minimum one representative of each Data Trust Member, which ensures that the development and deployment of the Data Trust adheres to the data, technical, and acceptable use specifications outlined in the exhibits attached hereto, in addition to managing, monitoring, and sustainability of the data trust.

- **"Data Trust Governance Board Representative"** shall mean the designated individual representing a Data Trust Member on the Data Trust Governance Board, who is empowered to vote on behalf of the Data Trust Member, if applicable. A Data Trust Governance Board Representative may be an employee of the Data Trust Member, or an employee of another organization, who has been delegated to perform this duty on behalf of the Data Trust Member.

- **"Data Trust Member"** shall mean an organization that is a party to this agreement and contributes one or more data resources it owns or controls (see "Member-owned Data Resources"), or does not contribute data, but is a stakeholder in the data trust and participates to fulfill an advisory function to the Governance Board, as defined in Section 5 of this agreement. Data Trust Members may include private companies, non-profit organizations, philanthropic and governmental entities, and community and/or advocacy groups as determined and approved by the data trust governance board.

- **"Data Trust Research Hub"** shall mean a permission based electronic portal providing approved Third Party Researchers access to Trust-managed data resources, as outlined in an approved Data Sharing Agreement between the Trustee, on behalf of all data trust Members, and the Third Party Researcher.

- **"Data Trust Technical Infrastructure"** shall mean any legal agreements, electronic registries, computer code, or other technology used to support, maintain, and govern the Data Trust, its Member-contributed Data Resources, and Trust-managed Data Resources. This may include extraction, transfer, and load ("ETL") scripts, databases, distributed ledgers, web applications, algorithms, authorization protocols, application programming interfaces ("APIs"), and compliance monitoring services.

- **"Data Trust User"** shall mean any organization, collaborative, initiative, or third party researcher that has expressly received permission by the Data Trust Governance Board to use specified trust-managed data resources for specified purposes.

- **"Data Security Classification"** shall mean the classification of data based on its level of sensitivity and the impact to the individual or organization represented by the data should that data be disclosed, altered, or

destroyed without authorization. An example of data security classification levels follows:

Classification Level

Description

Public (Lowest risk)

Applies to information assets that will not result in injury to individuals, governments or private sector institutions; and financial loss will be insignificant.

Protected A (Minimal risk)

Applies to information assets that, if compromised, could cause injury to an individual, organization or government.

Protected B (Moderate risk)

Applies to information assets that, if compromised, could cause serious injury to an individual organization or government.

Protected C (Significant risk)

Applies to information assets that, if compromised, could cause extremely grave injury to an individual, organization or government.

Examples of Risk Impact

1. Public (Lowest risk)

- No or minimal inconvenience if not available
- No or minimal impact if lost or altered

3. Protected B (Moderate risk)

- Loss of reputation or competitive advantage
- Loss of confidence in the program
- Loss of personal or individual privacy
- Loss of trade secrets or intellectual property
- Loss of opportunity (e.g., insurance, health coverage)
- Financial loss

2. Protected A (Minimal risk)

- Unfair competitive advantage
- Disruption to business if not available or inaccessible

4. Protected C (Significant risk)

- Loss of life
- Loss of public safety
- Significant Financial loss
- Destruction of partnerships and relationships
- Significant damage
- Sabotage/terrorism

- **"Derived Data"** shall mean any data or information that is a result of combining, aggregating, or otherwise processing the shared data via calculation combining, aggregating, or otherwise processing the shared data via calculation.

- **"Member-contributed Data Resources"** shall mean any data owned by or stewarded over by Member or other Data Trust Members provided to the Trustee for use by the Data Trust, and described in Exhibit D attached hereto or in the Data Trust electronic registry of Exhibit D.

- **"Personal Information"** (also known as personally identifiable information or "PII") shall mean any information, recorded or otherwise, relating to an identifiable individual. Almost any information, if linked to an identifiable individual, can become personal in nature.

- **"Raw Data"** shall mean data that has not yet been processed, altered, or combined with other data to form new data or metrics.

- **"Research Hub Review Committee"** shall mean the committee of Data Trust Member representatives tasked with reviewing research proposals based on Data Trust approved criteria, and making recommendations for approval.

- **"Sensitive Personal Information"** refers to information about an individual that must be protected from unauthorized access to safeguard the privacy or security of an individual, such as health or financial information.

- **"Trustee"** shall mean the Data Trust Member that has been approved by the Data Trust Governance Board to be the "trustee" of the data trust, responsible for ensuring that the data trust technical infrastructure adheres to the legal and technical specifications articulated in the Data Trust member agreement, and for carrying out subsequent decisions related to the Data Trust made by the Data Trust Governance Board.

- **"Trustee Affiliate"** shall mean any organization contracted to provide or assist in services related to Data Trust Technical Infrastructure on behalf of the Data Trust. Trustee Affiliate shall not be construed as a Member of the Data Trust and has no rights or responsibilities as such. Trustee Affiliate shall not be construed as a Member of the Data Trust and has no rights or responsibilities as such.

- **"Trust-managed Data Resource"** shall be any data resource, including derived or aggregate data, generated by the combination of one or more Member-contributed Data Resources and managed on behalf of the Trust by Technical Trustee or its Affiliates in support of the agreed upon goals of the Trust, or one or more of the Approved Projects and Uses.

Chapter 3

Data Trust Member Responsibilities

A. Data Trust Members ("Members") agree to clearly identify and label member-contributed data resources provided to Trustee for use by the Data Trust hereunder with the appropriate data security classification level. Members agree to update and maintain the classification of their member-contributed data resources as needed.

B. Members will collectively agree, via the Governance Board, on the data security classification levels to be used by the data trust.

C. Members agree to defend and hold harmless the Data Trust and Trustee as well as their respective trustees, officers, agents, and employees from any damages, liabilities, claims, and expenses (including reasonable attorney's fees) that result from the mislabeling of data provided to Trustee hereunder.

D. Members shall be responsible for obtaining all necessary consents and otherwise complying with all applicable laws and other rules and regulations prior to sharing personal information with the Trustee for use by the Data Trust. Necessary consents may include, but not be limited to consent for personal information to be used for research purposes, if research is an approved use of member-contributed data resources and/or trust-managed data resources.

E. Members represent and warrant that they have secured all necessary approvals from any third parties, such as organizations or individuals from which the data originates (if applicable), and have the legal right to provide Trustee personal information in acting on behalf of the Data Trust for the purposes contemplated by this agreement. Further, Members assume all responsibility for damages and costs to the extent resulting from its breach of the representation and warranty.

F. Members shall transmit, have access to, and have the ability to request removal at any time all data contributed to the Data Trust. Removal of Member-contributed Data Resources will occur within the timeframe of removal request agreed upon by the Governance Board .

G. Members shall have the ability to change or revoke access and use of member-contributed data resources at any time.Access may be revoked at the field, row, or element level and on a user-by-user basis.

H. Members may share additional data with the Trustee for use by the Data Trust at any time.

I. Members will designate a Data Trust Governance Board ("Governance Board") representative to participate in Data Trust Governance responsibilities, as written in Section 5 herein. Members may alternatively delegate its representation to another Data Trust Member's Data Trust Governance Board representative.

J. If Members classify data as public (or the equivalent) and public access of public data is listed as an Approved Use, Members acknowledge that once public data is contributed by any member, Trustee shall have the right to immediately make public data publicly available as approved and specified herein.

K. Members acknowledge and agree that their member-contributed data resources may be combined with those of other Data Trust Member organizations. All data, including copies of data, provided by Members to the Data Trust will be stored, maintained, and monitored using the agreed upon secure Data Trust Technical Infrastructure. Members shall be able to access the complete audit log of all access and use of data stored on Data Trust Technical Infrastructure at any time.

Chapter 4

Trustee Responsibilities

A. Trustee is responsible for providing the necessary legal, technical, and organizational infrastructure to support the creation, use, and maintenance of the Data Trust. In conjunction with the Data Trust Governance Board, Trustee will also ensure all Members, Users, Trustee and Trustee Affiliates are in compliance with the terms and conditions written herein.

B. If data is classified as public (or the equivalent) and public access of public data is listed as an Approved Use, once public data is contributed by any member, Trustee shall have the right to immediately make public data publicly available as approved and specified herein.

C. Trustee agrees to keep all member-contributed data resources deemed by Member to be sensitive and/or personal information, and classified accordingly, from disclosure by any unauthorized party.

D. Trustee agrees to only disclose member-contributed data resources to its employees and/or Trustee Affiliates who need access in order to meet Trustee's obligations and requirements for the purposes contemplated by this Agreement. Further, Trustee represents and certifies that no Data Trust Member nor Third Party shall have access to Members' member-contributed data resources in their raw form without express written or electronic approval by Member.

E. Trustee will ensure that no data identified and classified as personal information will be included in any published data.

F. Trustee will ensure Members have the opportunity to inspect aggregate trust-managed data resources to verify no data classified as sensitive or personal information is included before such data is published.

G. Trustee's designated Governance Board representative will serve as Chair of the Governance Board.

Chapter 5

Trustee Affiliate Responsibilities

A. Trustee Affiliate, at the direction of the Trustee, is responsible for configuring and deploying the technical infrastructure necessary for integrating member-contributed data resources for the purpose of creating trust-managed data resources. The technical infrastructure will adhere to the specifications detailed in Exhibit H attached hereto.

B. Trustee Affiliate, at the direction of the Trustee, will provide all DAGs, Methods, and Algorithms for the Data Trust Infrastructure to the Trustee to be documented in Exhibit E of this document.

C. Trustee Affiliate, at the direction of the Trustee, will limit access to raw member-contributed data resources and any data resources classified as sensitive to only its employees which need to access the data in order to configure or deploy the technical infrastructure.

D. Trustee Affiliate, at the direction of the Trustee, will secure all raw data, personal information, and data classified as sensitive via encryption both while the data is in transit and at rest.

E. At the request of one or more Governance Board representatives, Trustee Affiliate may attend meetings of the Governance Board in an advisory capacity and/or to provide technical or subject matter expertise. Trustee Affiliate shall not be construed as a Member of the Data Trust, and shall not have a vote on the Governance Board.

F. Upon termination of its engagement with the data trust, Trustee Affiliate will terminate its ability to access all member-contributed and trust-managed data resources.

Chapter 6

Data Trust Governance Board

A. Designated representative(s) of Members, along with Trustee's designated representative(s) collectively form the Data Trust Governance Board ("Governance Board").

B. The Governance Board responsibilities include, but are not limited to, overseeing the Data Trust to ensure that it is developed and managed in accordance with this Agreement, adopting a data security classification framework to be used for all Member-contributed and Trust-managed data resources, approving Trust-managed data resource access and use, developing necessary policies and privacy standards for Trust-managed data resources, creating and overseeing Subcommittees to address specific Data Trust needs or issues, and selecting and overseeing the Trustee in its duties in accordance with this Agreement.

C. The Governance Board is chaired by the Trustee's Governance Board representative. The Governance Board chair is responsible for scheduling Governance Board meetings, maintaining the list of Governance Board members, maintaining record of Governance Board vote tallies and decisions, and other duties as needed.

D. By default, each Data Trust Member, including the Trustee, has one equal vote on the Governance Board regardless of its number of Governance Board representatives. The Governance Board may, however, vote to classify non-data contributing members as "non-voting" and/or "advisory" only as identified in Exhibit B attached hereto. Members contributing data to the Data Trust may not have their voting rights revoked by the Governance Board or by any other party or means. Any Governance Board representative representing more than one voting Member must vote or abstain once on behalf of each Member they are representing.

E. An electronic registry of all Governance Board representatives shall be maintained by the Governance Board chair and updated at the request of any Member.

F. Sub-committees may be formed and disbanded at the pleasure of the Governance Board. The Governance Board shall authorize Sub-committee action, including whether decisions of the Subcommittee are binding without Governance Board review, or must be reviewed by the Governance Board before becoming official. Sub-committee membership must consist of at least one Governance Board representative, other members shall be nominated by Governance Board representatives and must be approved by the Governance Board.

Chapter 7

Academic Research as a Project or Approved Use

A. The Data Trust may, in this Agreement or through a future vote of the Governance Board, approve academic research as an approved use of the Trust-managed Data Resources. If approved, the Trustee shall make available a secure Data Trust Research Hub ("Research Hub") for access by approved researchers, for approved research, and put in place a process for certifying academic researchers for access to Trust-managed Data Resources through the Research Hub. This Research Hub may be managed by the Trustee or Trustee Affiliate(s). Approved uses, including approved academic research, shall be documented under Allowable Uses of Exhibit C attached hereto.

B. Individual researchers or research institutions ("Third Party Researcher") may submit a proposal for the use of Trust-managed Data Resources that include personal information or sensitive personal information. This proposal must be approved in writing or by electronic approval process conducted by Trustee and Governance Board.

C. Prior to accessing any data via the Research Hub or any other means, Third Party Researchers will be required to execute a Data Trust researcher agreement with the Trustee on behalf of the Data Trust that stipulates the permissions, use, and analyses approved, including timeline and publications. Further, Trustee or Trustee Affiliate(s) will provide prior written or electronic notice via Member's electronic portal that their data will be used by such Third Party Researcher as described in the Researcher data sharing agreement. Member may notify Trustee at any time to revoke such Third Party Researcher's access to the data.

D. Prior to being approved for access to the Research Hub, Third Party Researchers shall sign a Data Trust researcher agreement and complete a required training course which covers the use of the Research Hub, allowable use of data

provided via the Research Hub, Third Party Researcher obligations to Members, ethical guidelines, reporting of accidental misuse, and research review prior to publication. This training will be detailed on the Research Hub's website and will be updated from time to time. Proof of training completion will be required prior to the issuing of Research Hub credentials.

E. Third Party Researcher shall be required to complete relevant IRB approval prior to approval for access and use of Trust-managed Data Resources for research.

F. The Governance Board may elect to establish a Research Hub Review Committee for the purposes of reviewing and approving Third Party Researchers and their respective proposals. Governance Board representatives will nominate Data Trust Member representatives including experienced researchers or other technical experts to participate on the Research Hub Review Committee. Governance Board representatives may also nominate representatives from relevant communities or local interest groups to participate. Research Hub Review Committee members must be approved by the Governance Board.

G. The Governance Board or the Research Hub Review Committee will periodically review and approve through unanimous vote categories of allowable uses of Trust-managed Data Resources by Third Party Researchers along with their associated responsibilities and restrictions.

H. The Governance Board or the Research Hub Review Committee will review and approve proposals for new categories of research uses on a quarterly basis.

I. The Trustee will register and make publicly available all approved Third Party Researchers and proposals.

J. Data Trust Members will retain the right to opt out of the use of their member-contributed data resources in any particular research project at any time.

Chapter 8

Publication of Research

A. A Third Party Researcher may publish the results of research as stipulated in their individual data use agreement with the Trustee, provided such publication does not disclose Confidential Information, Member-contributed Data Resources or Trust-managed Data Resources classified as sensitive or personally identifiable information.

B. Data that has been aggregated by the Third Party Researcher may be published in accordance with other Unrestricted Data as determined by the Governance Board. However, prior to any such publication, Member and all other Data Trust Members which contribute data used in the creation of aggregate data shall be able review the aggregated data to verify no Restricted Data or Highly Restricted data is revealed.

C. A Third Party Researcher shall agree that, prior to submission of a manuscript describing any results for publication, they will share the manuscript with the Trustee and the Trustee shall forward to all Data Trust Members a copy of the manuscript to be submitted.

D. Members shall have thirty (30) days to determine whether a patent application or other intellectual property protection should be sought prior to the Third Party Researcher publishing their results in order to protect the Member's proprietary interests in any product or invention developed in connection with the Third Party Researcher's approved research proposal.

E. The Trustee agrees to withhold approving publication for an additional sixty (60) business days, if required, to allow Members to obtain patent protection. Upon the expiration of the sixty (60) business days, the Trustee shall allow the Third Party Researcher to submit the manuscript and publish results in any manner consistent with academic standards.

Chapter 9

Proprietary Rights

A. Member shall maintain ownership over any methodologies and code developed using only its own data, except for the code, software, or algorithms developed by the Trustee or its Affiliate(s) specific to Member data necessary to support and maintain the Trust and approved Projects and Uses.

B. To the extent practicable, Trustee and Trustee Affiliate(s) will release all software and algorithms developed or managed under Projects and Uses, as described in Exhibit C attached hereto, on behalf of the Trust as open source software unless otherwise determined by a vote of the Governance Board. In the event such software cannot be made available as open source software due to technical or other limitations, Trustee shall grant Member a non-exclusive, royalty-free license to use the software for the purposes set forth in Exhibit C attached hereto. Notwithstanding anything to the contrary, Trustee is not required to license or incorporate anything into software that Trustee reasonably believes would infringe another Member's intellectual property rights or that Trustee is not authorized to license.

C. Approved Third Party Researchers and other approved third party users shall maintain ownership over any methodologies developed during the course of their approved Projects and Uses, unless otherwise agreed upon by all Parties.

D. The Trustee, Third Party Researchers, and third-party users agree that, prior to release of any computer code, Trustee, Third Party Researchers, and/or third-party users shall, to the extent practicable, provide to the Member a copy of the code to ensure it contains no sensitive data.

E. All developments, discoveries, inventions, improvements, and modifications (whether or not patentable) conceived and reduced to practice in carrying out Projects and Uses conducted under this Agreement (the "Inventions") will be promptly disclosed by each Party to the other Party. Inventions made solely by employees, agents, consultants, independent contractors or other representatives

of the Trustee or its Affiliates will be solely owned by Trustee. Inventions made solely by employees, agents, consultants or other representatives of Member, will be owned solely by Member. Inventions made jointly by employees, agents, consultants, independent contractors or other representatives of the Trustee or its Affiliates, and/or employees, agents, consultants or other representatives of Member will be owned jointly by the jointly contributing Parties.

F. This Agreement does not transfer from one Party to the other any intellectual property rights that existed prior to this Agreement or that are created independently of this Agreement.

Chapter 10

Liability

Each Party represents and certifies that:

A. It has the right and necessary corporate authority to enter into this Agreement.

B. It has obtained all necessary consents, waivers, and permission to fulfil the purposes contemplated by this Agreement. For the avoidance of doubt, Member shall be solely responsible for obtaining all necessary consents and otherwise complying with applicable law in transmitting data to the Trustee and to permit the Trustee to perform its obligations pursuant to this Agreement.

C. ANY DERIVED DATA, AGGREGATE DATA, TRUST-OWNED DATA, AND RESEARCH OUTPUTS CREATED UNDER THIS AGREEMENT ARE PROVIDED "AS IS". THE TRUSTEE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE WORK OR PRODUCTS OF WORK CREATED UNDER THIS AGREEMENT, INCLUDING ANY EXPRESS OR IMPLIED WARRANTIES OF NON-INFRINGEMENT, OWNERSHIP, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE OF THE DATA GENERATION, RESEARCH OR ANY INVENTION OR PRODUCT.

D. Each party shall be responsible for its negligent acts or omissions and the negligent acts or omissions of its officers, directors, employees, and Affiliates to the extent allowed by law. Except with respect to: (i) either Party's breach of applicable law, or (ii) any Party's negligence or willful misconduct, no Party shall be liable hereunder for consequential, exemplary, or punitive damages (including lost profits or savings).

E. Any parties found to be non-compliant with the terms of this Agreement may have their Data Trust membership and/or their access to and their ability to use trust-managed data resources suspended or revoked. If Membership is

revoked, non-compliant Member may choose to have their associated member-contributed data resources removed from the Data Trust.

Chapter 11

Confidentiality

A. In performance of this Agreement, the Parties may disclose to each other, either in writing or orally, information which the disclosing Party deems to be proprietary and/or confidential (hereinafter, "Confidential Information") and not shared with the Trust, but may be necessary for the Trustee to perform its duties. Such information shall be marked "proprietary" or "confidential" by the disclosing Party.

B. Confidential Information shall be maintained in confidence during the term of this Agreement and for a period of three (3) years following the termination of this Agreement, except to the extent that it is required to be disclosed by law, regulation or judicial or administrative process. Data destruction and/or return procedures will be agreed upon by the Governance Board before any such data is shared, and documented in Exhibit H attached hereto. After such time, Confidential Information shall be destroyed or returned per the terms described in Exhibit H hereto.

C. In such a case where legal notice of disclosure is received, the Trustee will advise the Member prior to disclosure so that the Member will have an opportunity to seek a protective order or other appropriate relief.

D. Member shall be responsible for disclosing their own data as required of them under relevant Federal or Provincial law.

E. No Party shall disclose Confidential Information to any third party, and each Party shall keep strictly confidential all Confidential Information of the other. Using reasonable means, each Party shall protect the confidentiality thereof with at least the same level of effort that it employs to protect the confidentiality of its own proprietary and confidential information of like importance. Each Party receiving any such Confidential Information of the other Party may, however, disclose any portion of the Confidential Information of the other Party to such representatives of the receiving Party as are engaged in a use permitted by this

Agreement and have a need to know such portion, provided that representatives: (i) are directed to treat such Confidential Information confidentially and not to use such Confidential Information other than as permitted hereby or subsequently approved by Member, and (ii) are subject to a legal duty to maintain the confidentiality thereof. No receiving Party shall use the Confidential Information of a disclosing Party except solely to the extent necessary in and during the performance of this Agreement, as expressly licensed hereunder, or subsequently through electronically approved updates to this Agreement by a disclosing party. The receiving Party shall be responsible for any improper use or disclosure of any of the disclosing Party's Confidential Information by any of the receiving Party's current or former representatives.

Chapter 12

Ethical Use

A. Parties agree to abide by the ethical principles included in Exhibit F hereto around data trust creation, management, and use. Violation of these ethical principles may result in immediate revocation of Trust membership, revocation of access and use by approved Researchers or Users, or revocation of Trustee status by Trust.

B. Trustee or Trustee Affiliate agrees to include all directed acyclic graphs (DAGs), methods, and algorithms in Exhibit E hereto, and maintain a publicly available DAGs, Methods, and Algorithms registry with plain language descriptions of all relevant algorithms and models used by Trustee or its Affiliates, Members, or other approved users for informing decision making by an individual or organization using any Trust-managed Data Resource to promote and maintain algorithmic transparency.

C. Ethical principles enumerated in this Agreement may be updated through unanimous vote by the Governance Board. Any approved changes or additions by the Governance Board are applicable to all Members, Trustee, Trustee Affiliate, and its Data Trust Users within thirty (30) days of modification. Trustee must update the online registry of ethical principles within 7 days of Governance Board approval and send electronic notice to all Members and Data Trust Users of the changes to the ethical obligations within 14 days of approval.

Chapter 13

Term and Termination

A. The initial term of this Agreement shall commence on the Effective Date and will remain in effect for two (2) years thereafter unless otherwise modified by mutual agreement. Any party may terminate this Agreement without cause upon thirty (30) days' prior written notice to the other party. Upon termination, member may elect to have the Trustee return or destroy their member-contributed data or allow the Trustee to continue to work with such data subject to the terms of this Agreement. Members may also renew Agreement and Trust Membership for an additional two (2) year period at any time via written or electronic communication with Trustee. Trustee will retain an electronic registry of the expiration date of the agreement for all Members and allow Members to renew participation electronically through the registry.

B. Notwithstanding anything contained in this Agreement to the contrary, each Members' obligations under this Agreement may be expressly subject to an annual appropriation being made by Member's governing board in an amount sufficient to allow Member to perform its obligations under this Agreement. If sufficient funds are not appropriated this Agreement may be terminated by any Party without penalty. Member's obligations under this Agreement do not constitute a general obligation for indebtedness or multiple year direct or indirect debt or other financial obligation whatsoever within the meaning of the Constitution or laws of the relevant State.

Chapter 14

Miscellaneous

A. **Amendments**. Except as otherwise expressly provided herein, this Agreement may not be modified, amended or altered in any way except by a written agreement signed by the Parties or electronic consent provided by Parties.

B. **Assignment**. No Party may assign this Agreement or delegate any of its duties, in whole or in part, without the prior written or electronic consent of the other party; provided, however, that: (i) the Trustee may assign this Agreement and delegate its duties to an Affiliate; and (ii) either Party may assign this Agreement to an entity that acquires all or substantially all of the assets or business of such Party. If any assignee refuses to be bound by all of the terms and obligations of this Agreement or if any assignment is made in breach of the terms of this Agreement, then such assignment shall be null and void and of no force or effect.

C. **Counterparts**. This Agreement may be executed in multiple counterparts, each of which shall be deemed an original and all of which together shall be deemed the same agreement.

D. **Force Majeure**. No Party shall be liable for any failure or delay in performing its obligations under this Agreement, or for any loss or damage resulting therefrom, due to acts of God, the public enemy, terrorist activities, riots, fires, and similar causes beyond such Party's control.

E. **Governing Law**. This Agreement shall be governed by and interpreted in accordance with the internal substantive laws of the primary province of residence of the Trustee.

F. **Publicity**. No Party shall make reference to the other Party in a press release or any other written statement in connection with the Project without the other Party's prior consent, which consent shall not be unreasonably withheld, if it is intended for use in the news media. If there is no notice or disapproval within 48 hours after delivery to the other party for its review, the material shall be

deemed approved. Notwithstanding the foregoing, Trustee shall be permitted to use Member's name in a list of Data Trust Members that may also include a brief description of the Trust goals and priorities.

Chapter 15

Survival

Articles 1-13 shall survive termination or expiration of this Agreement for any reason.

Chapter 16

Signatures

IN WITNESS WHEREOF, the Parties hereto have executed this Agreement in duplicate by proper persons thereunto duly authorized.

Data Trust Members

Signed By

Date

Signatue

Member 1

Member 2

Member 3

Member 4

Exhibit A

Data Trust Parties

Parties to the Trust at time of signing are:

Parties to the trust can be added, removed, and updated according to the governance rules defined in EXHIBIT B.

An electronic registry of EXHIBIT A that enumerates all current Parties to the Data Trust is found at [Parties Registry Url]

Exhibit B

Data Trust Governance Board Structure and Procedures

[Trustee should include agreed upon Governance Board Procedures including, but not limited to, Governance Board and sub-committee configurations and structures, voting requirements and procedures, escalation procedures,]

Exhibit C

Data Trust Goals, Projects, and Allowable Uses

Goals

[Data Trust Members should include Goals for the Data Trust]

Projects

[Data Trust Members should include approved Projects for the Data Trust]

Allowable Uses

[Data Trust Members should include Allowable Uses for member-contributed data and/or trust-managed data resources]

An electronic registry of Exhibit C Data Trust Goals, Projects and Allowable Uses is maintained and updated [inse

Exhibit D

Member-Contributed Data Resources

[This section will be completed by Data Trust Members when they have an understanding of the data elements they will be contributing to the Data Trust]

Member-contributed Data Resource

Source of Data

Security Classification

Description of Data Resource

Resource 1

Resource 2

Resource 3

Table Definitions

A. **"Member-contributed Data Resource"**: Data elements being provided by Members

B. **"Description of Data Resource"**: Metadata associated with the Data Resource, such as defintion, format, etc.

An electronic registry of EXHIBIT D Member-contributed Data Resources at [insert Data Trust Member-contributed Data Resources Registry URL]

Exhibit E

Trust-Managed Data Resource Description

[This section will be completed by Trustee as Trust-managed Data Resources are approved by the Governance Board]

An electronic registry of EXHIBIT E is maintained and updated at [insert Data Trust-managed Resource Registry URL]

Exhibit F

Approved Users, Uses, and Access Levels

Application Developers, Researchers, Institutes, and Consortia

[Data Trust Members should insert any approved users, uses, and access levels for their member-contributed data Resources. Trustee should do so for Trust-managed Data Resources.]

User Name

Data Trust Resource

Access Level

Approved Use

Name 1

Name 2

Name 3

An electronic registry of EXHIBIT F is maintained and updated at [insert Data Trust User Registry URL]

Exhibit G

Directed Acyclic Graphs (DAGs), Methods, and Algorithms

[If Data Trust Members currently have Directed Acylic Graphs (DAGs), Methods, Algorithms, and/or Anonymization procedures or criteria, insert those in this section. Trustee or Affiliate will insert DAGs, Methods, and Algorithms for the Data Trust Infrastructure.]

An electronic registry of EXHIBIT G is maintained and updated at [insert Data Trust DAGs, Methods, and Algorithms Registry URL]

Exhibit H

Description of Data Trust Infrastructure, Technical Specifications, and Personal Informatio Procedures

[The Data Trust Trustee and/or the Trustee Affiliate(s), if applicable, will include description of Data Trust Infrastructure, Technical Specifications, and Procedures for protecting Personal Information, including collecting, aggregating, anonymizing and sharing Personal Information here]

An electronic version of EXHIBIT H is maintained and updated at [insert Data Trust Infrastructure, Technical Specifications, and PII Procedures URL]

Exhibit I

Additional Conditions, Memoranda of Understanding, or Data Use Agreements Governing Member-Contributed Data

[Data Trust Members should include copies of any existing Memoranda of Understanding, or Data Use Agreements governing Member-contributed Data Resources between Data Trust Members, Trustees and/or Affiliate(s)]

An electronic version of EXHIBIT H is maintained and updated at [insert MOU/DUA Registry URL]

Exhibt J

Data Trust Ethical Principles

[Data Trust Members should review Exhibit F and provide feedback on current ethical principles as well as include additional Ethical Principles]

Values

The Data Trust including, Trustee, Members, and Approved Users, commit to the following key values in developing and maintaining the Data Trust-managed Data Resources, Projects, and Allowable Uses.

Fairness

Understand, mitigate and communicate the presence of bias in both data practice and consumption.

Benefit

Set people before data and be responsible for maximizing social benefit and minimizing harm.

Openness

Practice humility and openness. Transparent practices, community engagement, and responsible communications are an integral part of data ethics.

Reliability

Ensure that every effort is made to glean a complete understanding of data, where it came from, and how it was created. Extend this effort for future users of all data and derivative data.

Data Trust Ethical Principles

All Data Trust Members, Trustee and Affiliates, researchers and other approved users commit to:

A. Consider collecting informed and purposeful consent of data subjects for all projects, regardless of legal requirements, and discard resulting data when that consent expires.

B. Make best effort to guarantee the security of data, subjects, and algorithms to prevent unauthorized access, disclosure of sensitive information, policy violations, tampering, or harm to data subjects.

C. Make best effort to protect anonymous data subjects, and any associated data, against any attempts to reverse-engineer, de-anonymize, or otherwise expose confidential information. * This includes all intermediate results, working with individuals or companies to help them maintain the anonymity of all data and parties involved, and supporting the rights to explanation, recourse, and rectification for any data subjects impacted by data work.

D. Practice responsible transparency as the default where possible, throughout the entire data lifecycle. * This includes providing enough context and documentation to enable other trained practitioners to understand and evaluate the use of data.

E. Foster diversity and openness by making efforts to ensure inclusion of participants from a variety of communities and socioeconomic backgrounds and with a broad representation of viewpoints. * This can be achieved by: being conscious of, and owning the results of actions, regardless of intent; promoting the voices of marginalized groups; acknowledging and self-checking privilege; accepting checks of privilege by others in good faith, and using privilege to advocate for equity. * The data community will not remain silent when witnessing others behaving in a manner that is not accessible, open, welcoming and inclusive.

F. Acknowledge and mitigate unfair bias throughout all aspects of data work. * This includes but is not limited to providing details and methodologies around data collection, processing and storage; and actively working to identify and disclose bias in algorithms, training data, and test data.

G. Make datasets with clearly established provenance the expected norm, rather than the exception. * As a data collector, be responsible for recording provenance; as a data publisher, be responsible for propagating provenance; as a data scientist, be responsible for reviewing, considering, and declaring what is known about data provenance. * Provenance is a living part of data work and can evolve with the project and all reasonable efforts should be made to understand and pass on provenance work.

H. Respect the needs of all stakeholders as they relate to privacy and data ownership.

I. Take great care to communicate clearly, responsibly and accessibly. * This includes: acknowledging and disclosing caveats and limitations to the process and outputs; considering and providing clear opportunities for feedback from all stakeholders; considering and discussing whether something should be done (not just if it can be done); and clearly identifying and communicating who may be impacted, and how they are impacted, in order to minimize any potential harm from data work.

J. Ensure that all data practitioners take responsibility for exercising ethical imagination in their work, including considering the implication of what came before and what may come after, and actively working to increase benefit and prevent harm to others.

OCAP® Committment

Additionally, all Data Trust Members, Trustee and Affiliates, researchers and other approved users commit to following The First Nations Principles of OCAP® when First Nations data is collected, protected, used, or shared.

There are four components of OCAP®: Ownership, Control, Access and Possession.

Ownership refers to the relationship of First Nations to their cultural knowledge, data, and information. This principle states that a community or group owns information collectively in the same way that an individual owns his or her personal information.

Control affirms that First Nations, their communities, and representative bodies are within their rights in seeking to control over all aspects of research and information management processes that impact them. First Nations control of research can include all stages of a particular research project-from start to finish. The principle extends to the control of resources and review processes, the planning process, management of the information and so on.

Access refers to the fact that First Nations must have access to information and data about themselves and their communities regardless of where it is held. The principle of access also refers to the right of First Nations communities and organizations to manage and make decisions regarding access to their collective information. This may be achieved, in practice, through standardized, formal protocols.

Possession While ownership identifies the relationship between a people and their information in principle, possession or stewardship is more concrete: it refers to the physical control of data. Possession is the mechanism by which ownership can be asserted and protected.

OCAP® is a registered trademark of the First Nations Information Governance Centre (FNIGC) www.FNIGC.ca/OCAP

[INSERT ADDITIONAL DATA TRUST ETHICAL PRINCIPLES]

An electronic registry of EXHIBIT F is maintained and updated at [insert Data Trust Ethical Principles Registry URL]

Exhibit K

Exhibits Change Managment Log

[Trustee shall include any additions or changes to Exhibits A, B, C, E, F, and H approved by the Governance Board. Members may make additions and/or changes to Exhibits D, G, and I at any time and such changes do not require approval of the Governance Board.]
